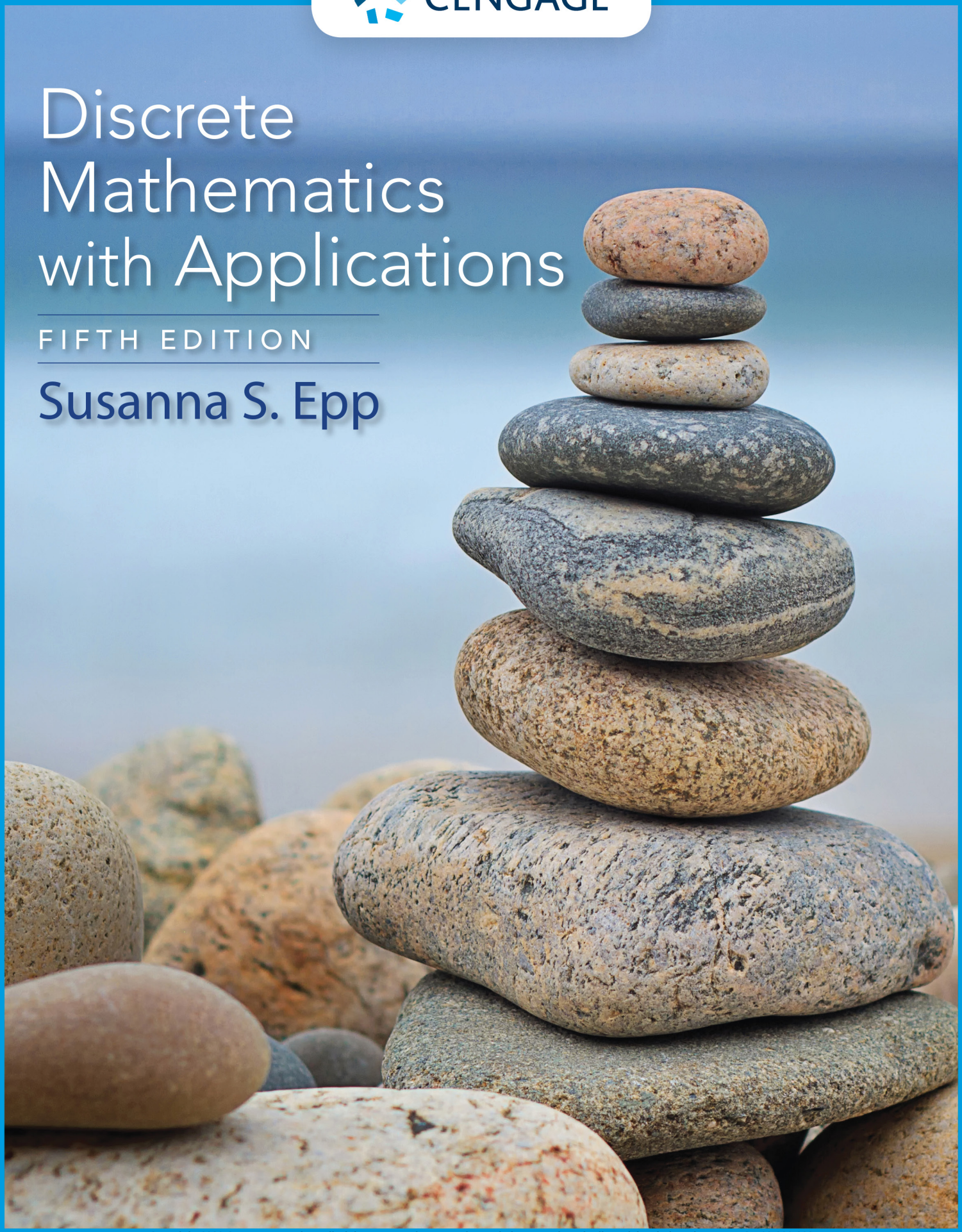
CENGAGE

Discrete Mathematics with Applications

FIFTH EDITION

Susanna S. Epp



DISCRETE MATHEMATICS
WITH APPLICATIONS

FIFTH EDITION

SUSANNA S. EPP
DePaul University

CENGAGE

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CENGAGE

Cover Photo: *The stones are discrete objects placed one on top of another like a chain of careful reasoning. A person who decides to build such a tower aspires to the heights and enjoys playing with a challenging problem. Choosing the stones takes both a scientific and an aesthetic sense. Getting them to balance requires patient effort and careful thought. And the tower that results is beautiful. A perfect metaphor for discrete mathematics!*

***Discrete Mathematics with Applications*, Fifth Edition**
Susanna S. Epp

Product Director: Mark Santee

Product Manager: Spencer Arritt

Learning Designer: Mona Zeftel, Laura Gallus

Content Manager: Lynh Pham, Christy Frame

Product Assistant: Amanda Rose

E2E Project Manager: Peggy Buskey

Marketing Manager: Shannon Hawkins, Giana Manzi

IP Analyst: Reba Frederics

IP Project Manager: Carly Belcher

Production Service: MPS Limited

Compositor: MPS Limited

Designer: Diana Graham

Cover Image: Katherine Gendreau Photography/Getty Images

Library of Congress Control Number: 2018953604

Student Edition:
ISBN: 978-1-337-69419-3

Loose-leaf Edition:
ISBN: 978-0-357-03523-8

Cengage
20 Channel Center Street
Boston, MA 02210
USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com**.

Cengage products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com**.

Printed in the United States of America
Print Number: 01 Print Year: 2018

To my husband, Helmut, and my children,
Amanda, Catherine, and Caroline

WEBASSIGN
From Cengage

STUDY SMARTER

Ever wonder if you studied enough? WebAssign from Cengage can help.

WebAssign is an online learning platform for your math, statistics and science courses. It helps you practice, focus your study time, and absorb what you learn. When class comes—you're way more confident.

With WebAssign you will:

Get instant feedback and grading

Know how well you understand concepts

Watch videos and tutorials when you're stuck

Perform better on in-class assignments

Ask your instructor today how you can get access to WebAssign!

cengage.com/webassign

Know if you're prepared for class!

93% correlation between homework scores and in-class performance

CONTENTS

PREFACE

My purpose in writing this book was to provide a clear, accessible treatment of discrete mathematics for students majoring or minoring in computer science, mathematics, mathematics education, and engineering. The goal of the book is to lay the mathematical foundation for computer science courses such as data structures, algorithms, relational database theory, automata theory and formal languages, compiler design, and cryptography, and for mathematics courses such as linear and abstract algebra, combinatorics, probability, logic and set theory, and number theory. By combining discussion of theory and practice, I have tried to show that mathematics has engaging and important applications as well as being interesting and beautiful in its own right.

A good background in algebra is the only prerequisite; the course may be taken by students either before or after a course in calculus. Previous editions of the book have been used successfully by students at hundreds of institutions in North and South America, Europe, the Middle East, Asia, and Australia.

Recent curricular recommendations from the Institute for Electrical and Electronic Engineers Computer Society (IEEE-CS) and the Association for Computing Machinery (ACM) include discrete mathematics as the largest portion of "core knowledge" for computer science students and state that students should take at least a one-semester course in the subject as part of their first-year studies, with a two-semester course preferred when possible. This book includes the topics recommended by those organizations and can be used effectively for either a one-semester or a two-semester course.

At one time, most of the topics in discrete mathematics were taught only to upper-level undergraduates. Discovering how to present these topics in ways that can be understood by first- and second-year students was the major and most interesting challenge of writing this book. The presentation was developed over a long period of experimentation during which my students were in many ways my teachers. Their questions, comments, and written work showed me what concepts and techniques caused them difficulty, and their reaction to my exposition showed me what worked to build their understanding and to encourage their interest. Many of the changes in this edition have resulted from continuing interaction with students.

Themes of a Discrete Mathematics Course

Discrete mathematics describes processes that consist of a sequence of individual steps. This contrasts with calculus, which describes processes that change in a continuous fashion. Whereas the ideas of calculus were fundamental to the science and technology of the industrial revolution, the ideas of discrete mathematics underlie the science and technology of the computer age. The main themes of a first course in discrete mathematics are logic and proof, induction and recursion, discrete structures, combinatorics and discrete probability, algorithms and their analysis, and applications and modeling.

Logic and Proof Probably the most important goal of a first course in discrete mathematics is to help students develop the ability to think abstractly. This means learning to use logically valid forms of argument and avoid common logical errors, appreciating what it means to reason from definitions, knowing how to use both direct and indirect arguments to derive new results from those already known to be true, and being able to work with symbolic representations as if they were concrete objects.

Induction and Recursion An exciting development of recent years has been the increased appreciation for the power and beauty of "recursive thinking." To think recursively means to address a problem by assuming that similar problems of a smaller nature have already been solved and figuring out how to put those solutions together to solve the larger problem. Such thinking is widely used in the analysis of algorithms, where recurrence relations that result from recursive thinking often give rise to formulas that are verified by mathematical induction.

Discrete Structures Discrete mathematical structures are the abstract structures that describe, categorize, and reveal the underlying relationships among discrete mathematical objects. Those studied in this book are the sets of integers and rational numbers, general sets, Boolean algebras, functions, relations, graphs and trees, formal languages and regular expressions, and finite-state automata.

Combinatorics and Discrete Probability Combinatorics is the mathematics of counting and arranging objects, and probability is the study of laws concerning the measurement of random or chance events. Discrete probability focuses on situations involving discrete sets of objects, such as finding the likelihood of obtaining a certain number of heads when an unbiased coin is tossed a certain number of times. Skill in using combinatorics and probability is needed in almost every discipline where mathematics is applied, from economics to biology, to computer science, to chemistry and physics, to business management.

Algorithms and Their Analysis The word *algorithm* was largely unknown in the middle of the twentieth century, yet now it is one of the first words encountered in the study of computer science. To solve a problem on a computer, it is necessary to find an algorithm, or step-by-step sequence of instructions, for the computer to follow. Designing an algorithm requires an understanding of the mathematics underlying the problem to be solved. Determining whether or not an algorithm is correct requires a sophisticated use of mathematical induction. Calculating the amount of time or memory space the algorithm will need in order to compare it to other algorithms that produce the same output requires knowledge of combinatorics, recurrence relations, functions, and O-, Ω-, and Θ-notations.

Applications and Modeling Mathematical topics are best understood when they are seen in a variety of contexts and used to solve problems in a broad range of applied situations. One of the profound lessons of mathematics is that the same mathematical model can be used to solve problems in situations that appear superficially to be totally dissimilar. A goal of this book is to show students the extraordinary practical utility of some very abstract mathematical ideas.

Special Features of This Book

Mathematical Reasoning The feature that most distinguishes this book from other discrete mathematics texts is that it teaches—explicitly but in a way that is accessible to

first- and second-year college and university students—the unspoken logic and reasoning that underlie mathematical thought. For many years I taught an intensively interactive transition-to-abstract-mathematics course to mathematics and computer science majors. This experience showed me that while it is possible to teach the majority of students to understand and construct straightforward mathematical arguments, the obstacles to doing so cannot be passed over lightly. To be successful, a text for such a course must address students' difficulties with logic and language directly and at some length. It must also include enough concrete examples and exercises to enable students to develop the mental models needed to conceptualize more abstract problems. The treatment of logic and proof in this book blends common sense and rigor in a way that explains the essentials, yet avoids overloading students with formal detail.

Spiral Approach to Concept Development A number of concepts in this book appear in increasingly more sophisticated forms in successive chapters to help students develop the ability to deal effectively with increasing levels of abstraction. For example, by the time students encounter the relatively advanced mathematics of Fermat's little theorem in Section 8.4, they have been introduced to the logic of mathematical discourse in Chapters 1, 2, and 3, learned the basic methods of proof and the concepts of *mod* and *div* in Chapter 4, explored *mod* and *div* as functions in Chapter 7, and become familiar with equivalence relations in Sections 8.2 and 8.3. This approach builds in useful review and develops mathematical maturity in natural stages.

Support for the Student Students at colleges and universities inevitably have to learn a great deal on their own. Though it is often frustrating, learning to learn through self-study is a crucial step toward eventual success in a professional career. This book has a number of features to facilitate students' transition to independent learning.

Worked Examples
The book contains over 500 worked examples, which are written using a problem-solution format and are keyed in type and in difficulty to the exercises. Many solutions for the proof problems are developed in two stages: first a discussion of how one might come to think of the proof or disproof and then a summary of the solution, which is enclosed in a box. This format allows students to read the problem and skip immediately to the summary, if they wish, only going back to the discussion if they have trouble understanding the summary. The format also saves time for students who are rereading the text in preparation for an examination.

Marginal Notes and Test Yourself Questions
Notes about issues of particular importance and cautionary comments to help students avoid common mistakes are included in the margins throughout the book. Questions designed to focus attention on the main ideas of each section are located between the text and the exercises. For convenience, the questions use a fill-in-the-blank format, and the answers are found immediately after the exercises.

Exercises
The book contains almost 2600 exercises. The sets at the end of each section have been designed so that students with widely varying backgrounds and ability levels will find some exercises they can be sure to do successfully and also some exercises that will challenge them.

Solutions for Exercises
To provide adequate feedback for students between class sessions, Appendix B contains at least one, and often several, complete solutions for every type of exercise

in the book. A blue exercise number indicates that there is a solution in Appendix B; the letter *H* is added for a solution that is less than complete. When two or more exercises use the same solution strategy, there is a full solution for the first and either another full solution or a partial solution for later ones. Exercises with several parts often have an answer and/or hint for one or more of the parts to help students determine whether they are on track so that they can make adjustments if needed.

Students are strongly urged not to consult solutions until they have tried their best to answer questions on their own. Once they have done so, however, comparing their answers with those given can lead to significantly improved understanding. There are also plenty of exercises without solutions to help students learn to grapple with mathematical problems in a realistic environment.

Reference Features

Many students have written me to say that the book helped them succeed in their advanced courses. One even wrote that he had used one edition so extensively that it had fallen apart, and he actually went out and bought a copy of the next edition, which he was continuing to use in a master's program. Figures and tables are included where doing so would help readers to a better understanding. In most, a second color is used to highlight meaning. My rationale for screening statements of definitions and theorems, for putting titles on exercises, and for giving the meanings of symbols and a list of reference formulas in the endpapers is to make it easier for students to use this book for review in a current course and as a reference in later ones.

Support for the Instructor I have received a great deal of valuable feedback from instructors who have used previous editions of this book. Many aspects of the book have been improved through their suggestions. In addition to the following items, there is additional instructor support on the book's website, described later in the preface.

Exercises

The large variety of exercises at all levels of difficulty allows instructors great freedom to tailor a course to the abilities of their students. Exercises with solutions in the back of the book have numbers in blue, and those whose solutions are given in a separate *Student Solutions Manual and Study Guide* have numbers that are a multiple of three. There are exercises of every type in the book that have no answer in either location so that instructors can assign whatever mixture they prefer of exercises with and without answers. The ample number of exercises of all kinds gives instructors a significant choice of problems to use for review assignments and exams. Instructors are invited to use the many exercises stated as questions rather than in "prove that" form to stimulate class discussion on the role of proof and counterexample in problem solving.

Flexible Sections

Most sections are divided into subsections so that an instructor can choose to cover certain subsections only and either omit the rest or leave them for students to study on their own. The division into subsections also makes it easier for instructors to break up sections if they wish to spend more than one day on them.

Presentation of Proof Methods

It is inevitable that most of the proofs and disproofs in this book will seem easy to instructors. Many students, however, find them difficult. In showing students how to discover and construct proofs and disproofs, I have tried to describe the kinds of approaches that mathematicians use when confronting challenging problems in their own research.

Complete Instructor Solutions

Complete instructor solutions to all exercises are available to anyone teaching a course from this book. They are available through the *Instructor's Companion Website*.

Highlights of the Fifth Edition

The changes made for this edition are based on suggestions from colleagues and other long-time users of previous editions, on continuing interactions with my students, and on developments within the evolving fields of computer science and mathematics.

Reorganization

- In response to instructor requests to move the introduction of certain topics earlier in the book, Section 1.2 now includes a definition and examples of strings. In addition, a new Section 1.4 contains definitions and examples of graphs and includes an introduction to graph coloring and the four-color theorem.
- The handshake theorem and its applications have been moved from Chapter 10 to Section 4.9. This gives students an early experience of using direct and indirect proof in a novel setting and was made possible because the elements of graph theory are now introduced in Chapter 1.

Improved Pedagogy

- The exposition has been reexamined throughout and carefully revised as needed.
- Exercises have been added for topics where students seemed to need additional practice, and they have been modified, as needed, to address student difficulties.
- Additional hints and full answers have been incorporated into Appendix B to give students more help for difficult topics.
- The introductory material in Chapter 4 was made more accessible by being divided into two sections. The first introduces basic concepts about proof and disproof in the context of elementary number theory, and the second adds examples and advice for writing proofs.

Logic and Applications

- Discussion was added about the role of bound variables and scope in mathematical writing and computer programming.
- The section on two's complements was significantly simplified.
- Language for expressing universal quantifiers was revised to provide a clearer basis for the idea of the generic particular in mathematical proof.
- The material on Boolean algebras was expanded.

Proof and Applications

- A greater variety of examples and exercises for number theory and set theory proofs is now included.
- The directions for writing proofs and the discussion of common mistakes have been revised and expanded in response to interaction with students.
- Discussion of historical background and recent mathematical results has been augmented.
- Material was added on using cryptographic hash functions to secure the transmission of digital data and on using cryptography to authenticate the sender of a transmitted message.

Induction and Recursion

- The sections on ordinary and strong mathematical induction were reorganized and expanded to increase the emphasis on applications.

- In the section on recursive definitions, the format used for proofs by structural induction was revised to parallel the format used for proofs by ordinary and strong mathematical induction. The set of examples and exercises illustrating recursive definitions and structural induction was significantly increased. The recursive definition for the set of strings over a finite set and for the length of a string were revised, and structural induction proofs for fundamental string properties are now included.

Graph Theory and the Analysis of Algorithm Efficiency

- Instructors who wish to give their students an early experience of graph theory can now do so by combining the introduction to graphs in Chapter 1 with the handshake theorem in Chapter 4.
- There is a new subsection on binary search trees in Chapter 10.
- The discussion of O-, Ω-, and Θ-notations was significantly simplified.
- Many exercises on algorithm efficiency were added or revised to make the concepts more accessible.

Student Resources

The *Student Companion Website* for this book includes:

- A general orientation for each chapter
- Review materials for each chapter
- Proof tips
- A link to the author's personal website, which contains errata information and links for interactive animations, tutorials, and other discrete mathematics resources on the Internet

Instructor's Resources

login.cengage.com

The *Instructor's Companion Website* for this book contains:

- Suggestions for how to approach the material of each chapter
- The *Complete Instructor's Solutions Manual*
- Ideas for projects and writing assignments
- Review materials to share with students
- Lecture Note PowerPoint slides
- Images from the book
- A test bank of questions for exams and quizzes
- Migration guide from 4th to 5th edition

Additional resources for the book are available at *http://condor.depaul.edu/sepp.*

WebAssign

www.webassign.com

WebAssign from Cengage *Discrete Mathematics with Applications,* Fifth Edition, is an online homework system, which instructors can choose to pair with the book. For students, it offers tutorial help in solving exercises, including review of relevant material, short instructional videos, and instant feedback on how they are doing. For instructors, it offers the ability to create customized homework sets, most of which are graded automatically and produce results directly into an online grade roster. Real-time access to their

students' performance makes it possible for instructors to adjust the presentation of material on an ongoing basis.

Student Solutions Manual and Study Guide

(ISBN: 978-0-357-03520-7)

In writing this book, I hoped that the exposition in the text, the worked examples, and the exercise solutions would provide all that a student would need to successfully master the material of the course. I continue to believe that any student who understands the solutions for all the exercises with complete solutions in Appendix B will have achieved an excellent command of the subject. Nonetheless, in response to requests for supplementary materials, I developed the *Student Solutions Manual and Study Guide*, available separately from the book, which contains complete solutions for all the exercises whose numbers are a multiple of 3. The guide also includes alternative explanations for some of the concepts and review questions for each chapter.

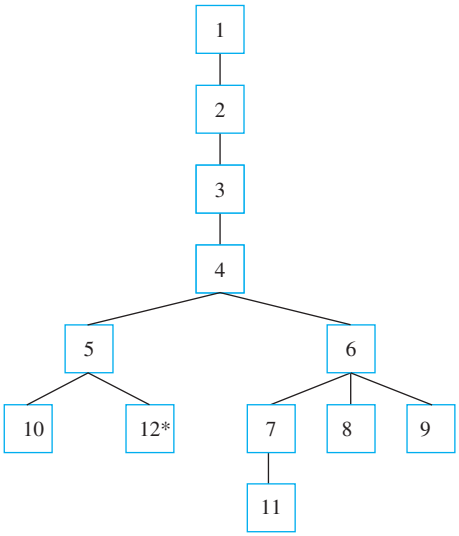
Organization

This book may be used effectively for a one- or two-semester course. Chapters contain core sections, sections covering optional mathematical material, and sections covering optional applications. Instructors have the flexibility to choose whatever mixture will best serve the needs of their students. The following table shows a division of the sections into categories.

Chapter	Core Sections	Sections Containing Optional Mathematical Material	Sections Containing Optional Computer Science Applications
1	1.1–1.3	1.4	1.4
2	2.1–2.3	2.5	2.4, 2.5
3	3.1–3.4	3.3	3.3
4	4.1–4.5, 4.7	4.6, 4.8, 4.9	4.10
5	5.1, 5.2, 5.6, 5.7	5.3, 5.4, 5.8	5.1, 5.5, 5.9
6	6.1	6.2–6.4	6.1, 6.4
7	7.1, 7.2	7.3, 7.4	7.1, 7.2, 7.4
8	8.1–8.3	8.4, 8.5	8.4, 8.5
9	9.1–9.4	9.5–9.9	9.3
10	10.1, 10.4	10.2, 10.3, 10.5	10.1, 10.4–10.6
11	11.1, 11.2	11.4	11.3, 11.5
12	12.1, 12.2	12.3	12.1–12.3

The following tree diagram shows, approximately, how the chapters of this book depend on each other. Chapters on different branches of the tree are sufficiently independent that instructors need to make at most minor adjustments if they skip chapters, or sections of chapters, but follow paths along branches of the tree.

In most cases, covering only the core sections of the chapters is adequate preparation for moving down the tree.



Acknowledgments

I owe a debt of gratitude to many people at DePaul University for their support and encouragement throughout the years I worked on editions of this book. A number of my colleagues used early versions and previous editions and provided many excellent suggestions for improvement. For this, I am thankful to Louis Aquila, J. Marshall Ash, Allan Berele, Jeffrey Bergen, William Chin, Barbara Cortzen, Constantine Georgakis, Sigrun Goes, Jerry Goldman, Lawrence Gluck, Leonid Krop, Carolyn Narasimhan, Walter Pranger, Eric Rieders, Ayse Sahin, Yuen-Fat Wong, and, most especially, Jeanne LaDuke. The thousands of students to whom I have taught discrete mathematics have had a profound influence on the presentation of the material in the book. By sharing their thoughts and thought processes with me, they taught me how to teach them better. I am very grateful for their help. I owe the DePaul University administration, especially deans, Charles Suchar, Michael Mezey, and Richard Meister, a special word of thanks for considering the writing of this book a worthwhile scholarly endeavor.

My thanks go to the reviewers for their valuable suggestions for this edition of the book: Naser Al-Hasan, Newberry College; Linda Fosnaugh, Midwestern State University; Robert Gessel, University of Akron; Juan Henriquez, University of New Orleans; Amy Hlavacek, Saginaw Valley State University; Kevin Lillis, Saint Ambrose University; Ramón Mata-Toledo, James Madison University; Bin Shao, University of San Francisco; Charles Qiao Zhang, Texas Christian University; and Cathleen Zucco-Teveloff, Rowan University. For their help with previous editions of the book, I am grateful to David Addis, Texas Christian University; Rachel Esselstein, California State University-Monterrey Bay; William Marion, Valparaiso University; Michael McClendon, University of Central Oklahoma; Steven Miller, Brown University; Itshak Borosh, Texas A & M University; Douglas M. Campbell, Brigham Young University; David G. Cantor, University of California at Los Angeles; C. Patrick Collier, University of Wisconsin-Oshkosh; Kevan H. Croteau, Francis Marion University; Irinel Drogan, University of Texas at Arlington; Pablo Echeverria, Camden County College; Henry A. Etlinger, Rochester Institute of Technology; Melvin J. Friske, Wisconsin Lutheran College; William Gasarch, University of Maryland; Ladnor

*Section 8.3 is needed for Section 12.3 but not for Sections 12.1 and 12.2.

Geissinger, University of North Carolina; Jerrold R. Griggs, University of South Carolina; Nancy Baxter Hastings, Dickinson College; Lillian Hupert, Loyola University Chicago; Joseph Kolibal, University of Southern Mississippi; Benny Lo, International Technological University; George Luger, University of New Mexico; Leonard T. Malinowski, Finger Lakes Community College; John F. Morrison, Towson State Unviersity; Paul Pederson, University of Denver; George Peck, Arizona State University; Roxy Peck, California Polytechnic State University, San Luis Obispo; Dix Pettey, University of Missouri; Anthony Ralston, State University of New York at Buffalo; Norman Richert, University of Houston-Clear Lake; John Roberts, University of Louisville; and George Schultz, St. Petersburg Junior College, Clearwater. Special thanks are due John Carroll, San Diego State University; Dr. Joseph S. Fulda; and Porter G. Webster, University of Southern Mississippi; Peter Williams, California State University at San Bernardino; and Jay Zimmerman, Towson University for their unusual thoroughness and their encouragement.

I have also benefitted greatly from the suggestions of the many instructors who have generously offered me their ideas for improvement based on their experiences with previous editions of the book, especially Jonathan Goldstine, Pennsylvania State University; David Hecker, St. Joseph's University; Edward Huff, Northern Virginia Community College; Robert Messer, Albion College; Sophie Quigley, Ryerson University; Piotr Rudnicki, University of Alberta; Anwar Shiek, Dine College; Norton Starr, Amherst College; Eng Wee, National University of Singapore; Doug Hogan, University of Illinois at Chicago; James Vanderhyde, Benedictine University; Ali Shaqlaih, University of North Texas at Dallas; Sam Needham, Diablo Valley College; Mohamed Aboutabl and Ramon A. Mata-Toledo, James Madison University; Larry Russ, Stevens Institute of Technology; Tomas Klos, Delft University; Margaret McQuain, Virginia Polytechnic Institute and State University; J. William Cupp, Indiana Wesleyan University; Jeffrey Mank, Framingham State University; Or Meir, University of Haifa; Audrey Julia Walegwa Mbogho, Pwani University, Kenya; Nariman Ammar, Birzeit University; Joshua T. Guerin, University of Tennessee at Martin; Jici Huang, Montana State University; Jerry Shi, University of Connecticut; Phuc Duong, Ton Duc Thang University, Vietnam; Abdul Rehman Abid, Iqra University, Pakistan; Yogesh More, SUNY Old Westbury; Mark Kaplan, Towson State University; Eric Neufeld, University of Saskatchewan; and Jeremy Tucker, Montana State University. Production of the third edition received valuable assistance from Christopher Novak, University of Michigan, Dearborn, and Ian Crewe, Ascension Collegiate School. For the third and fourth editions I am grateful for the many excellent suggestions for improvement made by Tom Jenkyns, Brock University, and for the fifth edition I am indebted to Roger Lipsett for his knowledgeable and careful attention to detail. I am also extremely grateful for the many appreciative messages I have received from students who have used previous editions of the book. They have inspired me to continue to find ever better ways to meet their needs in this edition, and I thank them for making the effort to contact me.

I owe many thanks to the Cengage staff, especially my editors, Laura Gallus, Mona Zeftel, Lynh Pham, and Spencer Arritt, for their thoughtful advice and reassuringly calm direction of the production process, and my previous editors, Dan Seibert, Stacy Green, Robert Pirtle, Barbara Holland, and Heather Bennett, for their encouragement and enthusiasm.

The older I get the more I realize the profound debt I owe my own mathematics teachers for shaping the way I perceive the subject. My first thanks must go to my husband, Helmut Epp, who, on a high school date (!), introduced me to the power and beauty of the field axioms and the view that mathematics is a subject with ideas as well as formulas and techniques. In my formal education, I am most grateful to Daniel Zelinsky and Ky Fan at Northwestern University and Izaak Wirszup, I. N. Herstein, and Irving Kaplansky at the

University of Chicago, all of whom, in their own ways, helped lead me to appreciate the elegance, rigor, and excitement of mathematics.

To my family, I owe thanks beyond measure. I am grateful to my mother, whose keen interest in the workings of the human intellect started me many years ago on the track that led ultimately to this book, and to my father, whose devotion to the written word has been a constant source of inspiration. I thank my children and grandchildren for their affection and cheerful acceptance of the demands this book has placed on my life. And, most of all, I am grateful to my husband, who for many years has encouraged me with his faith in the value of this project and supported me with his love and his wise advice.

Susanna Epp

CHAPTER 1 SPEAKING MATHEMATICALLY

Therefore O students study mathematics and do not build without foundations. —Leonardo da Vinci (1452–1519)

The aim of this book is to introduce you to a mathematical way of thinking that can serve you in a wide variety of situations. Often when you start work on a mathematical problem, you may have only a vague sense of how to proceed. You may begin by looking at examples, drawing pictures, playing around with notation, rereading the problem to focus on more of its details, and so forth. The closer you get to a solution, however, the more your thinking has to crystallize. And the more you need to understand, the more you need language that expresses mathematical ideas clearly, precisely, and unambiguously.

This chapter will introduce you to some of the special language that is a foundation for much mathematical thought, the language of variables, sets, relations, and functions. Think of the chapter like the exercises you would do before an important sporting event. Its goal is to warm up your mental muscles so that you can do your best.

1.1 Variables

A variable is sometimes thought of as a mathematical "John Doe" because you can use it as a placeholder when you want to talk about something but either (1) you imagine that it has one or more values but you don't know what they are, or (2) you want whatever you say about it to be equally true for all elements in a given set, and so you don't want to be restricted to considering only a particular, concrete value for it. To illustrate the first use, consider asking

> Is there a number with the following property: doubling it and adding 3 gives the same result as squaring it?

In this sentence you can introduce a variable to replace the potentially ambiguous word "it":

> Is there a number x with the property that $2x + 3 = x^2$?

The advantage of using a variable is that it allows you to give a temporary name to what you are seeking so that you can perform concrete computations with it to help discover its possible values. To emphasize the role of the variable as a placeholder, you might write the following:

> Is there a number $\square$ with the property that $2 \cdot \square + 3 = \square^2$?

The emptiness of the box can help you imagine filling it in with a variety of different values, some of which might make the two sides equal and others of which might not.

In this sense, a variable in a computer program is similar to a mathematical variable because it creates a location in computer memory (either actual or virtual) into which values can be placed.

To illustrate the second use of variables, consider the statement

> No matter what number might be chosen, if it is greater than 2, then its square is greater than 4.

In this case introducing a variable to give a temporary name to the (arbitrary) number you might choose enables you to maintain the generality of the statement, and replacing all instances of the word "it" by the name of the variable ensures that possible ambiguity is avoided:

> No matter what number n might be chosen, if n is greater than 2, then n^2 is greater than 4.

Example 1.1.1 **Writing Sentences Using Variables**

Use variables to rewrite the following sentences more formally.

a. Are there numbers with the property that the sum of their squares equals the square of their sum?

b. Given any real number, its square is nonnegative.

Solution

Note In part (a) the answer is yes. For instance, $a = 1$ and $b = 0$ would work. Can you think of other numbers that would also work?

a. Are there numbers a and b with the property that $a^2 + b^2 = (a + b)^2$?
Or: Are there numbers a and b such that $a^2 + b^2 = (a + b)^2$?
Or: Do there exist any numbers a and b such that $a^2 + b^2 = (a + b)^2$?

b. Given any real number r, r^2 is nonnegative.
Or: For any real number r, $r^2 \geq 0$.
Or: For every real number r, $r^2 \geq 0$. ■

Some Important Kinds of Mathematical Statements

Three of the most important kinds of sentences in mathematics are universal statements, conditional statements, and existential statements:

A **universal statement** says that a certain property is true for all elements in a set. (For example: *All positive numbers are greater than zero.*)

A **conditional statement** says that if one thing is true then some other thing also has to be true. (For example: *If 378 is divisible by 18, then 378 is divisible by 6.*)

Given a property that may or may not be true, an **existential statement** says that there is at least one thing for which the property is true. (For example: *There is a prime number that is even.*)

In later sections we will define each kind of statement carefully and discuss all of them in detail. The aim here is for you to realize that combinations of these statements can be expressed in a variety of different ways. One way uses ordinary, everyday language and another expresses the statement using one or more variables. The exercises are designed to help you start becoming comfortable in translating from one way to another.

Universal Conditional Statements

Universal statements contain some variation of the words "for every" and conditional statements contain versions of the words "if-then." A **universal conditional statement** is a statement that is both universal and conditional. Here is an example:

For every animal a, if a is a dog, then a is a mammal.

One of the most important facts about universal conditional statements is that they can be rewritten in ways that make them appear to be purely universal or purely conditional. For example, the previous statement can be rewritten in a way that makes its conditional nature explicit but its universal nature implicit:

If a is a dog, then a is a mammal.

Or: If an animal is a dog, then the animal is a mammal.

The statement can also be expressed so as to make its universal nature explicit and its conditional nature implicit:

For every dog a, a is a mammal.
Or: All dogs are mammals.

The crucial point is that the ability to translate among various ways of expressing universal conditional statements is enormously useful for doing mathematics and many parts of computer science.

Example 1.1.2 **Rewriting a Universal Conditional Statement**

Fill in the blanks to rewrite the following statement:

For every real number x, if x is nonzero then x^2 is positive.

a. If a real number is nonzero, then its square _____.

Note If you introduce x in the first part of the sentence, be sure to include it in the second part of the sentence.

b. For every nonzero real number x, _____.

c. If x _____, then _____.

d. The square of any nonzero real number is _____.

e. All nonzero real numbers have _____.

Solution

a. is positive

b. x^2 is positive

c. is a nonzero real number; x^2 is positive

d. positive

e. positive squares (*or*: squares that are positive) ■

Universal Existential Statements

A **universal existential statement** is a statement that is universal because its first part says that a certain property is true for all objects of a given type, and it is existential because its second part asserts the existence of something. For example:

Note For a number b to be an additive inverse for a number a means that $a + b = 0$.

Every real number has an additive inverse.

In this statement the property "has an additive inverse" applies universally to all real numbers. "Has an additive inverse" asserts the existence of something—an additive inverse—for each real number. However, the nature of the additive inverse depends on the real number; different real numbers have different additive inverses. Knowing that an additive inverse is a real number, you can rewrite this statement in several ways, some less formal and some more formal:*

All real numbers have additive inverses.
Or: For every real number r, there is an additive inverse for r.
Or: For every real number r, there is a real number s such that s is an additive inverse for r.

Introducing names for the variables simplifies references in further discussion. For instance, after the third version of the statement you might go on to write: When r is positive, s is negative, when r is negative, s is positive, and when r is zero, s is also zero.

One of the most important reasons for using variables in mathematics is that it gives you the ability to refer to quantities unambiguously throughout a lengthy mathematical argument, while not restricting you to consider only specific values for them.

Example 1.1.3 **Rewriting a Universal Existential Statement**

Fill in the blanks to rewrite the following statement: Every pot has a lid.

a. All pots _____.

b. For every pot P, there is _____.

c. For every pot P, there is a lid L such that _____.

Solution

a. have lids

b. a lid for P

c. L is a lid for P ■

Existential Universal Statements

An **existential universal statement** is a statement that is existential because its first part asserts that a certain object exists and is universal because its second part says that the object satisfies a certain property for all things of a certain kind. For example:

There is a positive integer that is less than or equal to every positive integer.

This statement is true because the number one is a positive integer, and it satisfies the property of being less than or equal to every positive integer. We can rewrite the statement in several ways, some less formal and some more formal:

Some positive integer is less than or equal to every positive integer.
Or: There is a positive integer m that is less than or equal to every positive integer.
Or: There is a positive integer m such that every positive integer is greater than or equal to m.
Or: There is a positive integer m with the property that for every positive integer n, $m \leq n$.

*A conditional could be used to help express this statement, but we postpone the additional complexity to a later chapter.

Example 1.1.4 **Rewriting an Existential Universal Statement**

Fill in the blanks to rewrite the following statement in three different ways:

> There is a person in my class who is at least as old as every person in my class.

a. Some _____ is at least as old as _____.

b. There is a person p in my class such that p is _____.

c. There is a person p in my class with the property that for every person q in my class, p is _____.

Solution

a. person in my class; every person in my class

b. at least as old as every person in my class

c. at least as old as q ■

Some of the most important mathematical concepts, such as the definition of limit of a sequence, can only be defined using phrases that are universal, existential, and conditional, and they require the use of all three phrases "for every," "there is," and "if-then." For example, if $a_1, a_2, a_3, \ldots$ is a sequence of real numbers, saying that

> the limit of a_n as n approaches infinity is L

means that

> **for every** positive real number ε, **there is** an integer N such that **for every** integer n, **if** $n > N$ **then** $-\varepsilon < a_n - L < \varepsilon$.

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. A universal statement asserts that a certain property is _____ for _____.
2. A conditional statement asserts that if one thing _____ then some other thing _____.
3. Given a property that may or may not be true, an existential statement asserts that _____ for which the property is true.

EXERCISE SET 1.1

Appendix B contains either full or partial solutions to all exercises with blue numbers. When the solution is not complete, the exercise number has an "***H***" next to it. A "*" next to an exercise number signals that the exercise is more challenging than usual. Be careful not to get into the habit of turning to the solutions too quickly. Make every effort to work exercises on your own before checking your answers. See the Preface for additional sources of assistance and further study.

In each of 1–6, fill in the blanks using a variable or variables to rewrite the given statement.

1. Is there a real number whose square is -1?
   a. Is there a real number x such that _____?
   b. Does there exist _____ such that $x^2 = -1$?
2. Is there an integer that has a remainder of 2 when it is divided by 5 and a remainder of 3 when it is divided by 6?
   a. Is there an integer n such that n has _____?
   b. Does there exist _____ such that if n is divided by 5 the remainder is 2 and if _____?

   Note: There are integers with this property. Can you think of one?
3. Given any two distinct real numbers, there is a real number in between them.

a. Given any two distinct real numbers a and b, there is a real number c such that c is _____.
b. For any two _____, _____ such that c is between a and b.

4. Given any real number, there is a real number that is greater.
a. Given any real number r, there is _____ s such that s is _____.
b. For any _____, _____ such that $s > r$.

5. The reciprocal of any positive real number is positive.
a. Given any positive real number r, the reciprocal of _____.
b. For any real number r, if r is _____, then _____.
c. If a real number r _____, then _____.

6. The cube root of any negative real number is negative.
a. Given any negative real number s, the cube root of _____.
b. For any real number s, if s is _____, then _____.
c. If a real number s _____, then _____.

7. Rewrite the following statements less formally, without using variables. Determine, as best as you can, whether the statements are true or false.
a. There are real numbers u and v with the property that $u + v < u - v$.
b. There is a real number x such that $x^2 < x$.
c. For every positive integer n, $n^2 \geq n$.
d. For all real numbers a and b, $|a + b| \leq |a| + |b|$.

In each of 8–13, fill in the blanks to rewrite the given statement.

8. For every object J, if J is a square then J has four sides.
a. All squares _____.
b. Every square _____.
c. If an object is a square, then it _____.
d. If J _____, then J _____.
e. For every square J, _____.

9. For every equation E, if E is quadratic then E has at most two real solutions.
a. All quadratic equations _____.
b. Every quadratic equation _____.
c. If an equation is quadratic, then it _____.
d. If E _____, then E _____.
e. For every quadratic equation E, _____.

10. Every nonzero real number has a reciprocal.
a. All nonzero real numbers _____.
b. For every nonzero real number r, there is _____ for r.
c. For every nonzero real number r, there is a real number s such that _____.

11. Every positive number has a positive square root.
a. All positive numbers _____.
b. For every positive number e, there is _____ for e.
c. For every positive number e, there is a positive number r such that _____.

12. There is a real number whose product with every number leaves the number unchanged.
a. Some _____ has the property that its _____.
b. There is a real number r such that the product of r _____.
c. There is a real number r with the property that for every real number s, _____.

13. There is a real number whose product with every real number equals zero.
a. Some _____ has the property that its _____.
b. There is a real number a such that the product of a _____.
c. There is a real number a with the property that for every real number b, _____.

ANSWERS FOR TEST YOURSELF

1. true; all elements of a set **2.** is true; also has to be true **3.** there is at least one thing

1.2 The Language of Sets

. . . when we attempt to express in mathematical symbols a condition proposed in words. First, we must understand thoroughly the condition. Second, we must be familiar with the forms of mathematical expression. —George Polyá (1887–1985)

Use of the word *set* as a formal mathematical term was introduced in 1879 by Georg Cantor (1845–1918). For most mathematical purposes we can think of a set intuitively, as

Cantor did, simply as a collection of elements. For instance, if C is the set of all countries that are currently in the United Nations, then the United States is an element of C, and if I is the set of all integers from 1 to 100, then the number 57 is an element of I.

Set-Roster Notation

If S is a set, the notation $x \in S$ means that x is an element of S. The notation $x \notin S$ means that x is not an element of S. A set may be specified using the **set-roster notation** by writing all of its elements between braces. For example, **{1, 2, 3}** denotes the set whose elements are 1, 2, and 3. A variation of the notation is sometimes used to describe a very large set, as when we write **{1, 2, 3, . . . , 100}** to refer to the set of all integers from 1 to 100. A similar notation can also describe an infinite set, as when we write **{1, 2, 3, . . . }** to refer to the set of all positive integers. (The symbol . . . is called an **ellipsis** and is read "and so forth.")

The **axiom of extension** says that a set is completely determined by what its elements are—not the order in which they might be listed or the fact that some elements might be listed more than once.

Example 1.2.1 **Using the Set-Roster Notation**

a. Let $A = \{1, 2, 3\}$, $B = \{3, 1, 2\}$, and $C = \{1, 1, 2, 3, 3, 3\}$. What are the elements of A, B, and C? How are A, B, and C related?

b. Is $\{0\} = 0$?

c. How many elements are in the set $\{1, \{1\}\}$?

d. For each nonnegative integer n, let $U_n = \{n, -n\}$. Find U_1, U_2, and U_0.

Solution

a. A, B, and C have exactly the same three elements: 1, 2, and 3. Therefore, A, B, and C are simply different ways to represent the same set.

b. $\{0\} \neq 0$ because $\{0\}$ is a set with one element, namely 0, whereas 0 is just the symbol that represents the number zero.

c. The set $\{1, \{1\}\}$ has two elements: 1 and the set whose only element is 1.

d. $U_1 = \{1, -1\}$, $U_2 = \{2, -2\}$, $U_0 = \{0, -0\} = \{0, 0\} = \{0\}$. ■

Certain sets of numbers are so frequently referred to that they are given special symbolic names. These are summarized in the following table.

Symbol	Set
R	the set of all real numbers
Z	the set of all integers
Q	the set of all rational numbers, or quotients of integers

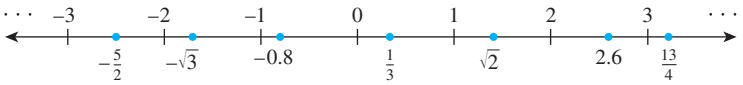
Note The **Z** is the first letter of the German word for integers, *Zahlen*. It stands for the *set* of all integers and should not be used as a shorthand for the word *integer*.

When the Symbols **R**, **Q**, and **Z** are handwritten, they appear as $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$.

Addition of a superscript + or − or the letters *nonneg* indicates that only the positive or negative or nonnegative elements of the set, respectively, are to be included. Thus $\mathbf{R}^+$ denotes the set of positive real numbers, and $\mathbf{Z}^{nonneg}$ refers to the set of nonnegative integers: 0, 1, 2, 3, 4, and so forth. Some authors refer to the set of nonnegative integers as the set of **natural numbers** and denote it as **N**. Other authors call only the positive

integers natural numbers. To prevent confusion, we simply avoid using the phrase *natural numbers* in this book.

The set of real numbers is usually pictured as the set of all points on a line, as shown below. The number 0 corresponds to a middle point, called the *origin*. A unit of distance is marked off, and each point to the right of the origin corresponds to a positive real number found by computing its distance from the origin. Each point to the left of the origin corresponds to a negative real number, which is denoted by computing its distance from the origin and putting a minus sign in front of the resulting number. The set of real numbers is therefore divided into three parts: the set of positive real numbers, the set of negative real numbers, and the number 0. *Note that 0 is neither positive nor negative*. Labels are given for a few real numbers corresponding to points on the line shown below.



The real number line is called *continuous* because it is imagined to have no holes. The set of integers corresponds to a collection of points located at fixed intervals along the real number line. Thus every integer is a real number, and because the integers are all separated from each other, the set of integers is called *discrete*. The name *discrete mathematics* comes from the distinction between continuous and discrete mathematical objects.

Another way to specify a set uses what is called the *set-builder notation*.

Note We read the left-hand brace as "the set of all" and the vertical line as "such that." In all other mathematical contexts, however, we do not use a vertical line to denote the words "such that"; we abbreviate "such that" as "s. t." or "s. th." or "∋."

Set-Builder Notation

Let S denote a set and let $P(x)$ be a property that elements of S may or may not satisfy. We may define a new set to be **the set of all elements x in S such that $P(x)$ is true**. We denote this set as follows:

$$\{x \in S \mid P(x)\}$$

the set of all — such that

Occasionally we will write $\{x \mid P(x)\}$ without being specific about where the element x comes from. It turns out that unrestricted use of this notation can lead to genuine contradictions in set theory. We will discuss one of these in Section 6.4 and will be careful to use this notation purely as a convenience in cases where the set S could be specified if necessary.

Example 1.2.2 **Using the Set-Builder Notation**

Given that $\mathbf{R}$ denotes the set of all real numbers, $\mathbf{Z}$ the set of all integers, and $\mathbf{Z}^+$ the set of all positive integers, describe each of the following sets.

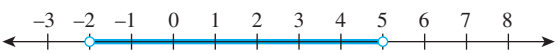
a. $\{x \in \mathbf{R} \mid -2 < x < 5\}$

b. $\{x \in \mathbf{Z} \mid -2 < x < 5\}$

c. $\{x \in \mathbf{Z}^+ \mid -2 < x < 5\}$

Solution

a. $\{x \in \mathbf{R} \mid -2 < x < 5\}$ is the open interval of real numbers (strictly) between -2 and 5. It is pictured as follows:



b. $\{x \in \mathbf{Z} \mid -2 < x < 5\}$ is the set of all integers (strictly) between -2 and 5. It is equal to the set $\{-1, 0, 1, 2, 3, 4\}$.

c. Since all the integers in $\mathbf{Z}^+$ are positive, $\{x \in \mathbf{Z}^+ \mid -2 < x < 5\} = \{1, 2, 3, 4\}$. ■

Subsets

A basic relation between sets is that of subset.

Definition

If A and B are sets, then A is called a **subset** of B, written $\boldsymbol{A \subseteq B}$, if, and only if, every element of A is also an element of B.

Symbolically:

$$A \subseteq B \quad \text{means that} \quad \text{for every element } x, \text{ if } x \in A \text{ then } x \in B.$$

The phrases *A is contained in B* and *B contains A* are alternative ways of saying that A is a subset of B.

It follows from the definition of subset that for a set A not to be a subset of a set B means that there is at least one element of A that is not an element of B. Symbolically:

$$A \not\subseteq B \quad \text{means that} \quad \text{there is at least one element } x \text{ such that } x \in A \text{ and } x \notin B.$$

Definition

Let A and B be sets. A is a **proper subset** of B if, and only if, every element of A is in B but there is at least one element of B that is not in A.

Example 1.2.3 **Subsets**

Let $A = \mathbf{Z}^+$, $B = \{n \in \mathbf{Z} \mid 0 \le n \le 100\}$, and $C = \{100, 200, 300, 400, 500\}$. Evaluate the truth and falsity of each of the following statements.

a. $B \subseteq A$

b. C is a proper subset of A

c. C and B have at least one element in common

d. $C \subseteq B$

e. $C \subseteq C$

Solution

a. False. Zero is not a positive integer. Thus zero is in B but zero is not in A, and so $B \not\subseteq A$.

b. True. Each element in C is a positive integer and, hence, is in A, but there are elements in A that are not in C. For instance, 1 is in A and not in C.

c. True. For example, 100 is in both C and B.

d. False. For example, 200 is in C but not in B.

e. True. Every element in C is in C. In general, the definition of subset implies that all sets are subsets of themselves. ■

Example 1.2.4 **Distinction between $\in$ and $\subseteq$**

Which of the following are true statements?

a. $2 \in \{1, 2, 3\}$ b. $\{2\} \in \{1, 2, 3\}$ c. $2 \subseteq \{1, 2, 3\}$

d. $\{2\} \subseteq \{1, 2, 3\}$ e. $\{2\} \subseteq \{\{1\}, \{2\}\}$ f. $\{2\} \in \{\{1\}, \{2\}\}$

Solution Only (a), (d), and (f) are true.

For (b) to be true, the set $\{1, 2, 3\}$ would have to contain the element $\{2\}$. But the only elements of $\{1, 2, 3\}$ are 1, 2, and 3, and 2 is not equal to $\{2\}$. Hence (b) is false.

For (c) to be true, the number 2 would have to be a set and every element in the set 2 would have to be an element of $\{1, 2, 3\}$. This is not the case, so (c) is false.

For (e) to be true, every element in the set containing only the number 2 would have to be an element of the set whose elements are $\{1\}$ and $\{2\}$. But 2 is not equal to either $\{1\}$ or $\{2\}$, and so (e) is false. ■

Cartesian Products

ArchivePL/Alamy Stock Photo

Kazimierz Kuratowski (1896–1980)

With the introduction of Georg Cantor's set theory in the late nineteenth century, it began to seem possible to put mathematics on a firm logical foundation by developing all of its various branches from set theory and logic alone. A major stumbling block was how to use sets to define an ordered pair because the definition of a set is unaffected by the order in which its elements are listed. For example, $\{a, b\}$ and $\{b, a\}$ represent the same set, whereas in an ordered pair we want to be able to indicate which element comes first.

In 1914 crucial breakthroughs were made by Norbert Wiener (1894–1964), a young American who had recently received his Ph.D. from Harvard, and the German mathematician Felix Hausdorff (1868–1942). Both gave definitions showing that an ordered pair can be defined as a certain type of set, but both definitions were somewhat awkward. Finally, in 1921, the Polish mathematician Kazimierz Kuratowski (1896–1980) published the following definition, which has since become standard. It says that an ordered pair is a set of the form

$$\{\{a\}, \{a, b\}\}.$$

This set has elements, $\{a\}$ and $\{a, b\}$. If $a \neq b$, then the two sets are distinct and a is in both sets whereas b is not. This allows us to distinguish between a and b and say that a is the first element of the ordered pair and b is the second element of the pair. If $a = b$, then we can simply say that a is both the first and the second element of the pair. In this case the set that defines the ordered pair becomes $\{\{a\}, \{a, a\}\}$, which equals $\{\{a\}\}$.

However, it was only long after ordered pairs had been used extensively in mathematics that mathematicians realized that it was possible to define them entirely in terms of sets, and, in any case, the set notation would be cumbersome to use on a regular basis. The usual notation for ordered pairs refers to $\{\{a\}, \{a, b\}\}$ more simply as (a, b).

Notation

Given elements a and b, the symbol (a, b) denotes the **ordered pair** consisting of a and b together with the specification that a is the first element of the pair and b is the second element. Two ordered pairs (a, b) and (c, d) are equal if, and only if, $a = c$ and $b = d$. Symbolically:

$$(a, b) = (c, d) \quad \text{means that} \quad a = c \text{ and } b = d.$$

Example 1.2.5 **Ordered Pairs**

a. Is $(1, 2) = (2, 1)$?

b. Is $\left(3, \frac{5}{10}\right) = \left(\sqrt{9}, \frac{1}{2}\right)$?

c. What is the first element of $(1, 1)$?

Solution

a. No. By definition of equality of ordered pairs,

$$(1, 2) = (2, 1) \text{ if, and only if, } 1 = 2 \text{ and } 2 = 1.$$

But $1 \neq 2$, and so the ordered pairs are not equal.

b. Yes. By definition of equality of ordered pairs,

$$\left(3, \frac{5}{10}\right) = \left(\sqrt{9}, \frac{1}{2}\right) \text{ if, and only if, } 3 = \sqrt{9} \text{ and } \frac{5}{10} = \frac{1}{2}.$$

Because these equations are both true, the ordered pairs are equal.

c. In the ordered pair $(1, 1)$, the first and the second elements are both 1. ■

The notation for an *ordered n-tuple* generalizes the notation for an ordered pair to a set with any finite number of elements. It also takes both order and multiplicity into account.

Definition

Let n be a positive integer and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elements. The **ordered *n*-tuple, $(x_1, x_2, \ldots, x_n)$**, consists of $x_1, x_2, \ldots, x_n$ together with the ordering: first x_1, then x_2, and so forth up to x_n. An ordered 2-tuple is called an **ordered pair**, and an ordered 3-tuple is called an **ordered triple**.

Two ordered n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ are **equal** if, and only if, $x_1 = y_1$, $x_2 = y_2, \ldots$, and $x_n = y_n$.

Symbolically:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \iff x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n.$$

Example 1.2.6 **Ordered *n*-tuples**

a. Is $(1, 2, 3, 4) = (1, 2, 4, 3)$?

b. Is $\left(3, (-2)^2, \frac{1}{2}\right) = \left(\sqrt{9}, 4, \frac{3}{6}\right)$?

Solution

a. No. By definition of equality of ordered 4-tuples,

$$(1, 2, 3, 4) = (1, 2, 4, 3) \iff 1 = 1, 2 = 2, 3 = 4, \text{ and } 4 = 3$$

But $3 \neq 4$, and so the ordered 4-tuples are not equal.

b. Yes. By definition of equality of ordered triples,

$$\left(3, (-2)^2, \frac{1}{2}\right) = \left(\sqrt{9}, 4, \frac{3}{6}\right) \iff 3 = \sqrt{9} \text{ and } (-2)^2 = 4 \text{ and } \frac{1}{2} = \frac{3}{6}.$$

Because these equations are all true, the two ordered triples are equal. ■

Definition

Given sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $A_1, A_2, \ldots, A_n$, denoted $\boldsymbol{A_1 \times A_2 \times \cdots \times A_n}$, is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1$, $a_2 \in A_2, \ldots, a_n \in A_n$.

Symbolically:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

In particular,

$$A_1 \times A_2 = \{(a_1, a_2) \mid a_1 \in A_1 \text{ and } a_2 \in A_2\}$$

is the Cartesian product of A_1 and A_2.

Example 1.2.7 **Cartesian Products**

Let $A = \{x, y\}$, $B = \{1, 2, 3\}$, and $C = \{a, b\}$.

a. Find $A \times B$.

b. Find $B \times A$.

c. Find $A \times A$.

d. How many elements are in $A \times B$, $B \times A$, and $A \times A$?

e. Find $(A \times B) \times C$

f. Find $A \times B \times C$

g. Let $\mathbf{R}$ denote the set of all real numbers. Describe $\mathbf{R} \times \mathbf{R}$.

Solution

a. $A \times B = \{(x, 1), (y, 1), (x, 2), (y, 2), (x, 3), (y, 3)\}$

b. $B \times A = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$

c. $A \times A = \{(x, x), (x, y), (y, x), (y, y)\}$

Note This is why it makes sense to call a Cartesian product a product!

d. $A \times B$ has 6 elements. Note that this is the number of elements in A times the number of elements in B. $B \times A$ has 6 elements, the number of elements in B times the number of elements in A. $A \times A$ has 4 elements, the number of elements in A times the number of elements in A.

e. The Cartesian product of A and B is a set, so it may be used as one of the sets making up another Cartesian product. This is the case for $(A \times B) \times C$.

$$\begin{aligned}(A \times B) \times C &= \{(u, v) \mid u \in A \times B \text{ and } v \in C\} \quad \text{by definition of Cartesian product} \\ &= \{((x, 1), a), ((x, 2), a), ((x, 3), a), ((y, 1), a), \\ &\quad ((y, 2), a), ((y, 3), a), ((x, 1), b), ((x, 2), b), ((x, 3), b), \\ &\quad ((y, 1), b), ((y, 2), b), ((y, 3), b)\}\end{aligned}$$

f. The Cartesian product $A \times B \times C$ is superficially similar to but is not quite the same mathematical object as $(A \times B) \times C$. $(A \times B) \times C$ is a set of ordered pairs of which one element is itself an ordered pair, whereas $A \times B \times C$ is a set of ordered triples. By definition of Cartesian product,

$$\begin{aligned} A \times B \times C &= \{(u, v, w) \mid u \in A, v \in B, \text{ and } w \in C\} \\ &= \{(x, 1, a), (x, 2, a), (x, 3, a), (y, 1, a), (y, 2, a), (y, 3, a), (x, 1, b), \\ &\quad (x, 2, b), (x, 3, b), (y, 1, b), (y, 2, b), (y, 3, b)\}. \end{aligned}$$

g. $\mathbf{R} \times \mathbf{R}$ is the set of all ordered pairs (x, y) where both x and y are real numbers. If horizontal and vertical axes are drawn on a plane and a unit length is marked off, then each ordered pair in $\mathbf{R} \times \mathbf{R}$ corresponds to a unique point in the plane, with the first and second elements of the pair indicating, respectively, the horizontal and vertical positions of the point. The term **Cartesian plane** is often used to refer to a plane with this coordinate system, as illustrated in Figure 1.2.1.

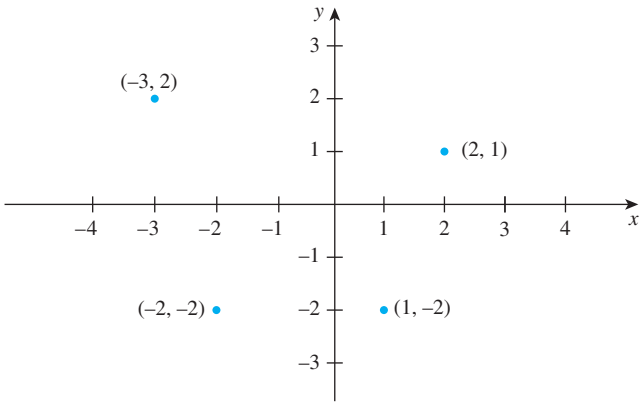


FIGURE 1.2.1 A Cartesian Plane ■

Another notation, which is important in both mathematics and computer science, denotes objects called *strings*.*

Definition

Let n be a positive integer. Given a finite set A, a **string of length n over A** is an ordered n-tuple of elements of A written without parentheses or commas. The elements of A are called the **characters** of the string. The **null string** over A is defined to be the "string" with no characters. It is often denoted λ and is said to have length 0. If $A = \{0, 1\}$, then a string over A is called a **bit string**.

Example 1.2.8 **Strings**

Let $A = \{a, b\}$. List all the strings of length 3 over A with at least two characters that are the same.

Solution

$$aab, aba, baa, aaa, bba, bab, abb, bbb$$

In computer programming it is important to distinguish among different kinds of data structures and to respect the notations that are used for them. Similarly in mathematics, it is important to distinguish among, say, $\{a, b, c\}$, $\{\{a, b\}, c\}$, (a, b, c), $(a, (b, c))$, abc, and so forth, because these are all significantly different objects. ■

*A more formal definition of string, using recursion, is given in Section 5.9.

TEST YOURSELF

1. When the elements of a set are given using the set-roster notation, the order in which they are listed _____.
2. The symbol $\mathbf{R}$ denotes _____.
3. The symbol $\mathbf{Z}$ denotes _____.
4. The symbol $\mathbf{Q}$ denotes _____.
5. The notation $\{x \mid P(x)\}$ is read _____.
6. For a set A to be a subset of a set B means that _____.
7. Given sets A and B, the Cartesian product $A \times B$ is _____.
8. Given sets A, B, and C, the Cartesian product $A \times B \times C$ is _____.
9. A string of length n over a set S is an ordered n-tuple of elements of S, written without _____ or _____.

EXERCISE SET 1.2

1. Which of the following sets are equal?

$$A = \{a, b, c, d\} \qquad B = \{d, e, a, c\}$$
$$C = \{d, b, a, c\} \qquad D = \{a, a, d, e, c, e\}$$

2. Write in words how to read each of the following out loud.
   a. $\{x \in \mathbf{R}^+ \mid 0 < x < 1\}$
   b. $\{x \in \mathbf{R} \mid x \leq 0 \text{ or } x \geq 1\}$
   c. $\{n \in \mathbf{Z} \mid n \text{ is a factor of } 6\}$
   d. $\{n \in \mathbf{Z}^+ \mid n \text{ is a factor of } 6\}$

3. a. Is $4 = \{4\}$?
   b. How many elements are in the set $\{3, 4, 3, 5\}$?
   c. How many elements are in the set $\{1, \{1\}, \{1, \{1\}\}\}$?

4. a. Is $2 \in \{2\}$?
   b. How many elements are in the set $\{2, 2, 2, 2\}$?
   c. How many elements are in the set $\{0, \{0\}\}$?
   d. Is $\{0\} \in \{\{0\}, \{1\}\}$?
   e. Is $0 \in \{\{0\}, \{1\}\}$?

H 5. Which of the following sets are equal?

$$A = \{0, 1, 2\}$$
$$B = \{x \in \mathbf{R} \mid -1 \leq x < 3\}$$
$$C = \{x \in \mathbf{R} \mid -1 < x < 3\}$$
$$D = \{x \in \mathbf{Z} \mid -1 < x < 3\}$$
$$E = \{x \in \mathbf{Z}^+ \mid -1 < x < 3\}$$

H 6. For each integer n, let $T_n = \{n, n^2\}$. How many elements are in each of T_2, T_{-3}, T_1, and T_0? Justify your answers.

7. Use the set-roster notation to indicate the elements in each of the following sets.
   a. $S = \{n \in \mathbf{Z} \mid n = (-1)^k, \text{ for some integer } k\}$.
   b. $T = \{m \in \mathbf{Z} \mid m = 1 + (-1)^i, \text{ for some integer } i\}$.
   c. $U = \{r \in \mathbf{Z} \mid 2 \leq r \leq -2\}$
   d. $V = \{s \in \mathbf{Z} \mid s > 2 \text{ or } s < 3\}$
   e. $W = \{t \in \mathbf{Z} \mid 1 < t < -3\}$
   f. $X = \{u \in \mathbf{Z} \mid u \leq 4 \text{ or } u \geq 1\}$

8. Let $A = \{c, d, f, g\}$, $B = \{f, j\}$, and $C = \{d, g\}$. Answer each of the following questions. Give reasons for your answers.
   a. Is $B \subseteq A$?
   b. Is $C \subseteq A$?
   c. Is $C \subseteq C$?
   d. Is C a proper subset of A?

9. a. Is $3 \in \{1, 2, 3\}$?
   b. Is $1 \subseteq \{1\}$?
   c. Is $\{2\} \in \{1, 2\}$?
   d. Is $\{3\} \in \{1, \{2\}, \{3\}\}$?
   e. Is $1 \in \{1\}$?
   f. Is $\{2\} \subseteq \{1, \{2\}, \{3\}\}$?
   g. Is $\{1\} \subseteq \{1, 2\}$?
   h. Is $1 \in \{\{1\}, 2\}$?
   i. Is $\{1\} \subseteq \{1, \{2\}\}$?
   j. Is $\{1\} \subseteq \{1\}$?

10. a. Is $((-2)^2, -2^2) = (-2^2, (-2)^2)$?
    b. Is $(5, -5) = (-5, 5)$?
    c. Is $(8 - 9, \sqrt[3]{-1}) = (-1, -1)$?
    d. Is $\left(\frac{-2}{-4}, (-2)^3\right) = \left(\frac{3}{6}, -8\right)$?

11. Let $A = \{w, x, y, z\}$ and $B = \{a, b\}$. Use the set-roster notation to write each of the following sets, and indicate the number of elements that are in each set.
    a. $A \times B$
    b. $B \times A$
    c. $A \times A$
    d. $B \times B$

12. Let $S = \{2, 4, 6\}$ and $T = \{1, 3, 5\}$. Use the set-roster notation to write each of the following sets, and indicate the number of elements that are in each set.
a. $S \times T$
b. $T \times S$
c. $S \times S$
d. $T \times T$

13. Let $A = \{1, 2, 3\}$, $B = \{u\}$, and $C = \{m, n\}$. Find each of the following sets.
a. $A \times (B \times C)$
b. $(A \times B) \times C$
c. $A \times B \times C$

14. Let $R = \{a\}$, $S = \{x, y\}$, and $T = \{p, q, r\}$. Find each of the following sets.
a. $R \times (S \times T)$
b. $(R \times S) \times T$
c. $R \times S \times T$

15. Let $S = \{0, 1\}$. List all the strings of length 4 over S that contain three or more 0's.

16. Let $T = \{x, y\}$. List all the strings of length 5 over T that have exactly one y.

ANSWERS FOR TEST YOURSELF

1. does not matter **2.** the set of all real numbers **3.** the set of all integers **4.** the set of all rational numbers **5.** the set of all x such that $P(x)$ **6.** every element in A is an element in B **7.** the set of all ordered pairs (a, b) where a is in A and b is in B **8.** the set of ordered triples of the form (a, b, c) where $a \in A$, $b \in B$, and $c \in C$ **9.** parentheses; commas

1.3 The Language of Relations and Functions

Mathematics is a language. —Josiah Willard Gibbs (1839–1903)

There are many kinds of relationships in the world. For instance, we say that two people are related by blood if they share a common ancestor and that they are related by marriage if one shares a common ancestor with the spouse of the other. We also speak of the relationship between student and teacher, between people who work for the same employer, and between people who share a common ethnic background.

Similarly, the objects of mathematics may be related in various ways. A set A may be said to be related to a set B if A is a subset of B, or if A is not a subset of B, or if A and B have at least one element in common. A number x may be said to be related to a number y if $x < y$, or if x is a factor of y, or if $x^2 + y^2 = 1$. Two identifiers in a computer program may be said to be related if they have the same first eight characters, or if the same memory location is used to store their values when the program is executed. And the list could go on!

Let $A = \{0, 1, 2\}$ and $B = \{1, 2, 3\}$ and let us say that an element x in A is related to an element y in B if, and only if, x is less than y. Let us use the notation $x\ R\ y$ as a shorthand for the sentence "x is related to y." Then

$$\begin{aligned} 0\ R\ 1 \quad &\text{since} \quad 0 < 1, \\ 0\ R\ 2 \quad &\text{since} \quad 0 < 2, \\ 0\ R\ 3 \quad &\text{since} \quad 0 < 3, \\ 1\ R\ 2 \quad &\text{since} \quad 1 < 2, \\ 1\ R\ 3 \quad &\text{since} \quad 1 < 3, \quad \text{and} \\ 2\ R\ 3 \quad &\text{since} \quad 2 < 3. \end{aligned}$$

On the other hand, if the notation $x \not R y$ represents the sentence "x is not related to y," then

$$1 \not R 1 \quad \text{since} \quad 1 \not< 1,$$
$$2 \not R 1 \quad \text{since} \quad 2 \not< 1, \quad \text{and}$$
$$2 \not R 2 \quad \text{since} \quad 2 \not< 2.$$

Recall that the Cartesian product of A and B, $A \times B$, consists of all ordered pairs whose first element is in A and whose second element is in B:

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

In this case,

$$A \times B = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}.$$

The elements of some ordered pairs in $A \times B$ are related, whereas the elements of other ordered pairs are not. Consider the set of all ordered pairs in $A \times B$ whose elements are related

$$\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}.$$

Observe that knowing which ordered pairs lie in this set is equivalent to knowing which elements are related to which. The relation itself can therefore be thought of as the totality of ordered pairs whose elements are related by the given condition. The formal mathematical definition of relation, based on this idea, was introduced by the American mathematician and logician C. S. Peirce in the nineteenth century.

Definition

Let A and B be sets. A **relation R from A to B** is a subset of $A \times B$. Given an ordered pair (x, y) in $A \times B$, **x is related to y by R**, written $x \, R \, y$, if, and only if, (x, y) is in R. The set A is called the **domain** of R and the set B is called its **co-domain**.

The notation for a relation R may be written symbolically as follows:

$$\boldsymbol{x \, R \, y} \quad \text{means that} \quad \boldsymbol{(x, y) \in R.}$$

The notation $x \not R y$ means that x is not related to y by R:

$$\boldsymbol{x \not R y} \quad \text{means that} \quad \boldsymbol{(x, y) \notin R.}$$

Example 1.3.1 **A Relation as a Subset**

Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ and define a relation R from A to B as follows: Given any $(x, y) \in A \times B$,

$$(x, y) \in R \quad \text{means that} \quad \frac{x - y}{2} \text{ is an integer.}$$

a. State explicitly which ordered pairs are in $A \times B$ and which are in R.

b. Is $1 \, R \, 3$? Is $2 \, R \, 3$? Is $2 \, R \, 2$?

c. What are the domain and co-domain of R?

Solution

a. $A \times B = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$. To determine explicitly the composition of R, examine each ordered pair in $A \times B$ to see whether its elements satisfy the defining condition for R.

$(1, 1) \in R$ because $\frac{1-1}{2} = \frac{0}{2} = 0$, which is an integer.

$(1, 2) \notin R$ because $\frac{1-2}{2} = \frac{-1}{2}$, which is not an integer.

$(1, 3) \in R$ because $\frac{1-3}{2} = \frac{-2}{2} = -1$, which is an integer.

$(2, 1) \notin R$ because $\frac{2-1}{2} = \frac{1}{2}$, which is not an integer.

$(2, 2) \in R$ because $\frac{2-2}{2} = \frac{0}{2} = 0$, which is an integer.

$(2, 3) \notin R$ because $\frac{2-3}{2} = \frac{-1}{2}$, which is not an integer.

Thus

$$R = \{(1, 1), (1, 3), (2, 2)\}$$

b. Yes, $1\ R\ 3$ because $(1, 3) \in R$.
No, $2 \not R\ 3$ because $(2, 3) \notin R$.
Yes, $2\ R\ 2$ because $(2, 2) \in R$.

c. The domain of R is $\{1, 2\}$ and the co-domain is $\{1, 2, 3\}$. ■

Example 1.3.2 **The Circle Relation**

Define a relation C from $\mathbf{R}$ to $\mathbf{R}$ as follows: For any $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$(x, y) \in C \quad \text{means that} \quad x^2 + y^2 = 1.$$

a. Is $(1, 0) \in C$? Is $(0, 0) \in C$? Is $\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in C$? Is $-2\ C\ 0$? Is $0\ C\ (-1)$? Is $1\ C\ 1$?

b. What are the domain and co-domain of C?

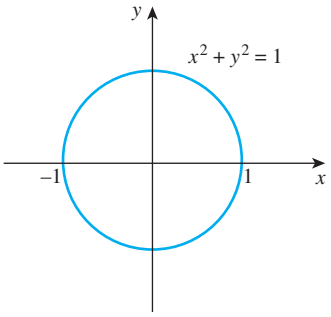
c. Draw a graph for C by plotting the points of C in the Cartesian plane.

Solution

a. Yes, $(1, 0) \in C$ because $1^2 + 0^2 = 1$.
No, $(0, 0) \notin C$ because $0^2 + 0^2 = 0 \neq 1$.
Yes, $\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in C$ because $\left(-\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{4} + \frac{3}{4} = 1$.
No, $-2 \not C\ 0$ because $(-2)^2 + 0^2 = 4 \neq 1$.
Yes, $0\ C\ (-1)$ because $0^2 + (-1)^2 = 1$.
No, $1 \not C\ 1$ because $1^2 + 1^2 = 2 \neq 1$.

b. The domain and co-domain of C are both $\mathbf{R}$, the set of all real numbers.

c.



■

Arrow Diagram of a Relation

Suppose R is a relation from a set A to a set B. The **arrow diagram for R** is obtained as follows:

1. Represent the elements of A as points in one region and the elements of B as points in another region.
2. For each x in A and y in B, draw an arrow from x to y if, and only if, x is related to y by R. Symbolically:

$$\begin{aligned} &\textbf{Draw an arrow from } x \textbf{ to } y \\ &\textbf{if, and only if,} \quad x\ R\ y \\ &\textbf{if, and only if,} \quad (x, y) \in R. \end{aligned}$$

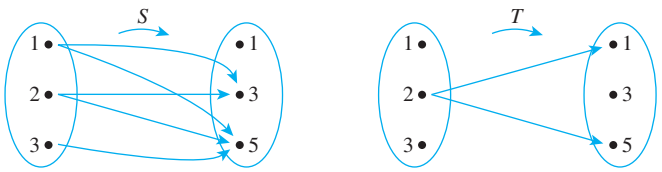
Example 1.3.3 **Arrow Diagrams of Relations**

Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3\}$ and define relations S and T from A to B as follows: For every $(x, y) \in A \times B$,

$$(x, y) \in S \quad \text{means that} \quad x < y \qquad S \text{ is a "less than" relation.}$$
$$T = \{(2, 1), (2, 5)\}.$$

Draw arrow diagrams for S and T.

Solution



These example relations illustrate that it is possible to have several arrows coming out of the same element of A pointing in different directions. Also, it is quite possible to have an element of A that does not have an arrow coming out of it. ■

Functions

In Section 1.2 we showed that ordered pairs can be defined in terms of sets and we defined Cartesian products in terms of ordered pairs. In this section we introduced relations as subsets of Cartesian products. Thus we can now define functions in a way that depends only on the concept of set. Although this definition is not obviously related to the way we usually work with functions in mathematics, it is satisfying from a theoretical point of view, and computer scientists like it because it is particularly well suited for operating with functions on a computer.

Definition

A **function F from a set A to a set B** is a relation with domain A and co-domain B that satisfies the following two properties:

1. For every element x in A, there is an element y in B such that $(x, y) \in F$.
2. For all elements x in A and y and z in B,

$$\text{if} \quad (x, y) \in F \text{ and } (x, z) \in F, \quad \text{then} \quad y = z.$$

Properties (1) and (2) can be stated less formally as follows: A relation F from A to B is a function if, and only if:

1. Every element of A is the first element of an ordered pair of F.
2. No two distinct ordered pairs in F have the same first element.

In most mathematical situations we think of a function as sending elements from one set, the domain, to elements of another set, the co-domain. Because of the definition of function, each element in the domain corresponds to one and only one element of the co-domain.

More precisely, if F is a function from a set A to a set B, then given any element x in A, property (1) from the function definition guarantees that there is at least one element of B that is related to x by F and property (2) guarantees that there is at most one such element. This makes it possible to give the element that corresponds to x a special name.

Function Notation

If A and B are sets and F is a function from A to B, then given any element x in A, the unique element in B that is related to x by F is denoted $\boldsymbol{F(x)}$, which is read "$\boldsymbol{F}$ **of** $\boldsymbol{x}$."

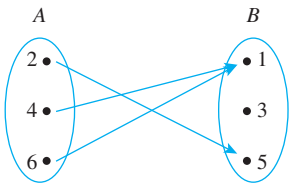
Example 1.3.4 **Functions and Relations on Finite Sets**

Let $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$. Which of the relations R, S, and T defined below are functions from A to B?

a. $R = \{(2, 5), (4, 1), (4, 3), (6, 5)\}$

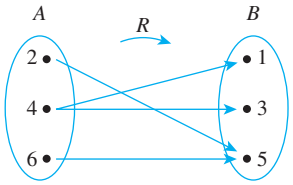
b. For every $(x, y) \in A \times B$, $(x, y) \in S$ means that $y = x + 1$.

c. T is defined by the arrow diagram

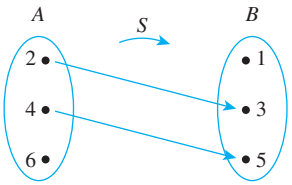


Solution

a. R is not a function because it does not satisfy property (2). The ordered pairs (4, 1) and (4, 3) have the same first element but different second elements. You can see this graphically if you draw the arrow diagram for R. There are two arrows coming out of 4: One points to 1 and the other points to 3.



b. S is not a function because it does not satisfy property (1). It is not true that every element of A is the first element of an ordered pair in S. For example, $6 \in A$ but there is no y in B such that $y = 6 + 1 = 7$. You can also see this graphically by drawing the arrow diagram for S.



Note In part (c), $T(4) = T(6)$. This illustrates the fact that although no element of the domain of a function can be related to more than one element of the co-domain, several elements in the domain can be related to the same element in the co-domain.

c. T is a function: Each element in $\{2, 4, 6\}$ is related to some element in $\{1, 3, 5\}$, and no element in $\{2, 4, 6\}$ is related to more than one element in $\{1, 3, 5\}$. When these properties are stated in terms of the arrow diagram, they become (1) there is an arrow coming out of each element of the domain, and (2) no element of the domain has more than one arrow coming out of it. So you can write $T(2) = 5$, $T(4) = 1$, and $T(6) = 1$. ■

Example 1.3.5 **Functions and Relations on Sets of Strings**

Let $A = \{a, b\}$ and let S be the set of all strings over A.

a. Define a relation L from S to $\mathbf{Z}^{nonneg}$ as follows: For every string s in S and for every nonnegative integer n,

$$(s, n) \in L \text{ means that the length of } s \text{ is } n.$$

Observe that L is a function because every string in S has one and only one length. Find $L(abaaba)$ and $L(bbb)$.

b. Define a relation C from S to S as follows: For all strings s and t in S,

$$(s, t) \in C \text{ means that } t = as,$$

where as is the string obtained by appending a on the left of the characters in s. (C is called **concatenation** by a on the left.) Observe that C is a function because every string in S consists entirely of a's and b's and adding an additional a on the left creates a new strong that also consists of a's and b's and thus is also in S. Find $C(abaaba)$ and $C(bbb)$.

Solution

a. $L(abaaba) = 6$ and $L(bbb) = 3$

b. $C(abaaba) = aabaaba$ and $C(bbb) = abbb$ ■

Function Machines

Another useful way to think of a function is as a machine. Suppose f is a function from X to Y and an input x of X is given. Imagine f to be a machine that processes x in a certain way to produce the output $f(x)$. This is illustrated in Figure 1.3.1.

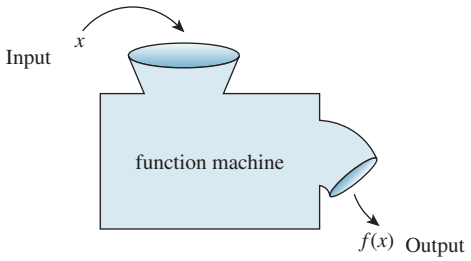


FIGURE 1.3.1

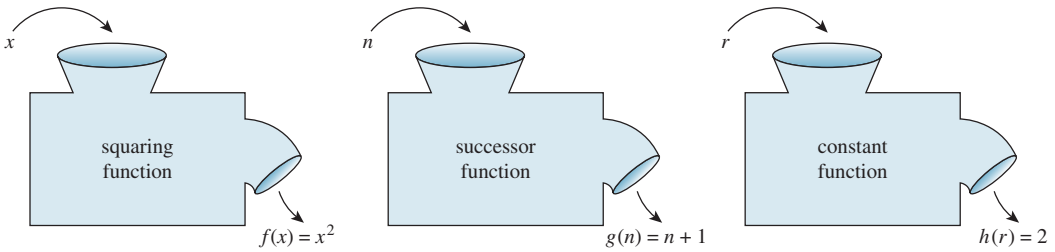
Example 1.3.6 **Functions Defined by Formulas**

The **squaring function** f from $\mathbf{R}$ to $\mathbf{R}$ is defined by the formula $f(x) = x^2$ for every real number x. This means that no matter what real number input is substituted for x, the output of f will be the square of that number. This idea can be represented by writing $f(\square) = \square^2$. In other words, f sends each real number x to x^2, or, symbolically, $f\colon x \longrightarrow x^2$. Note that the variable x is a dummy variable; any other symbol could replace it, as long as the replacement is made everywhere the x appears.

The **successor function** g from $\mathbf{Z}$ to $\mathbf{Z}$ is defined by the formula $g(n) = n + 1$. Thus, no matter what integer is substituted for n, the output of g will be that number plus 1: $g(\square) = \square + 1$. In other words, g sends each integer n to $n + 1$, or, symbolically, $g\colon n \longrightarrow n + 1$.

An example of a **constant function** is the function h from $\mathbf{Q}$ to $\mathbf{Z}$ defined by the formula $h(r) = 2$ for all rational numbers r. This function sends each rational number r to 2. In other words, no matter what the input, the output is always 2: $h(\square) = 2$ or $h\colon r \longrightarrow 2$.

The functions f, g, and h are represented by the function machines in Figure 1.3.2.



(a) (b) (c)

FIGURE 1.3.2 ■

A function is an entity in its own right. It can be thought of as a certain relationship between sets or as an input/output machine that operates according to a certain rule. This is the reason why a function is generally denoted by a single symbol or string of symbols, such as f, G, of log, or sin.

A relation is a subset of a Cartesian product and a function is a special kind of relation. Specifically, if f and g are functions from a set A to a set B, then

$$f = \{(x, y) \in A \times B \mid y = f(x)\} \quad \text{and} \quad g = \{(x, y) \in A \times B \mid y = g(x)\}.$$

It follows that

> ***f* equals *g***, written $f = g$, if, and only if, $f(x) = g(x)$ for all x in A.

Example 1.3.7 **Equality of Functions**

Define functions f and g from $\mathbf{R}$ to $\mathbf{R}$ by the following formulas:

$$f(x) = |x| \quad \text{for every } x \in \mathbf{R}.$$
$$g(x) = \sqrt{x^2} \quad \text{for every } x \in \mathbf{R}.$$

Does $f = g$?

Solution

Yes. Because the absolute value of any real number equals the square root of its square, $|x| = \sqrt{x^2}$ for all $x \in \mathbf{R}$. Hence $f = g$. ■

TEST YOURSELF

1. Given sets A and B, a relation from A to B is _____.
2. A function F from A to B is a relation from A to B that satisfies the following two properties:
   a. for every element x of A, there is _____.
   b. for all elements x in A and y and z in B, if _____ then _____.
3. If F is a function from A to B and x is an element of A, then $F(x)$ is _____.

EXERCISE SET 1.3

1. Let $A = \{2, 3, 4\}$ and $B = \{6, 8, 10\}$ and define a relation R from A to B as follows: For every $(x, y) \in A \times B$,

   $$(x, y) \in R \quad \text{means that} \quad \frac{y}{x} \text{ is an integer.}$$

   a. Is $4\ R\ 6$? Is $4\ R\ 8$? Is $(3, 8) \in R$? Is $(2, 10) \in R$?
   b. Write R as a set of ordered pairs.
   c. Write the domain and co-domain of R.
   d. Draw an arrow diagram for R.

2. Let $C = D = \{-3, -2, -1, 1, 2, 3\}$ and define a relation S from C to D as follows: For every $(x, y) \in C \times D$,

   $$(x, y) \in S \quad \text{means that} \quad \frac{1}{x} - \frac{1}{y} \text{ is an integer.}$$

   a. Is $2\ S\ 2$? Is $-1\ S\ -1$? Is $(3, 3) \in S$? Is $(3, -3) \in S$?
   b. Write S as a set of ordered pairs.
   c. Write the domain and co-domain of S.
   d. Draw an arrow diagram for S.

3. Let $E = \{1, 2, 3\}$ and $F = \{-2, -1, 0\}$ and define a relation T from E to F as follows: For every $(x, y) \in E \times F$,

   $$(x, y) \in T \quad \text{means that} \quad \frac{x - y}{3} \text{ is an integer.}$$

   a. Is $3\ T\ 0$? Is $1\ T\ (-1)$? Is $(2, -1) \in T$? Is $(3, -2) \in T$?
   b. Write T as a set of ordered pairs.
   c. Write the domain and co-domain of T.
   d. Draw an arrow diagram for T.

4. Let $G = \{-2, 0, 2\}$ and $H = \{4, 6, 8\}$ and define a relation V from G to H as follows: For every $(x, y) \in G \times H$,

   $$(x, y) \in V \quad \text{means that} \quad \frac{x - y}{4} \text{ is an integer.}$$

   a. Is $2\ V\ 6$? Is $(-2)\ V\ (8)$? Is $(0, 6) \in V$? Is $(2, 4) \in V$?
   b. Write V as a set of ordered pairs.
   c. Write the domain and co-domain of V.
   d. Draw an arrow diagram for V.

5. Define a relation S from $\mathbf{R}$ to $\mathbf{R}$ as follows: For every $(x, y) \in \mathbf{R} \times \mathbf{R}$,

   $$(x, y) \in S \quad \text{means that} \quad x \geq y.$$

   a. Is $(2, 1) \in S$? Is $(2, 2) \in S$? Is $2\ S\ 3$? Is $(-1)\ S\ (-2)$?
   b. Draw the graph of S in the Cartesian plane.

6. Define a relation R from $\mathbf{R}$ to $\mathbf{R}$ as follows: For every $(x, y) \in \mathbf{R} \times \mathbf{R}$,

   $$(x, y) \in R \quad \text{means that} \quad y = x^2.$$

   a. Is $(2, 4) \in R$? Is $(4, 2) \in R$? Is $(-3)\ R\ 9$? Is $9\ R\ (-3)$?
   b. Draw the graph of R in the Cartesian plane.

7. Let $A = \{4, 5, 6\}$ and $B = \{5, 6, 7\}$ and define relations R, S, and T from A to B as follows: For every $(x, y) \in A \times B$:

   $(x, y) \in R$ means that $x \geq y$.

   $(x, y) \in S$ means that $\frac{x - y}{2}$ is an integer.

   $T = \{(4, 7), (6, 5), (6, 7)\}$.

   a. Draw arrow diagrams for R, S, and T.
   b. Indicate whether any of the relations R, S, and T are functions.

8. Let $A = \{2, 4\}$ and $B = \{1, 3, 5\}$ and define relations U, V, and W from A to B as follows: For every $(x, y) \in A \times B$:

   $(x, y) \in U$ means that $y - x > 2$.

   $(x, y) \in V$ means that $y - 1 = \frac{x}{2}$.

   $W = \{(2, 5), (4, 1), (2, 3)\}$.

   a. Draw arrow diagrams for U, V, and W.
   b. Indicate whether any of the relations U, V, and W are functions.

9. **a.** Find all functions from $\{0, 1\}$ to $\{1\}$.
b. Find two relations from $\{0, 1\}$ to $\{1\}$ that are not functions.

10. Find four relations from $\{a, b\}$ to $\{x, y\}$ that are not functions from $\{a, b\}$ to $\{x, y\}$.

11. Let $A = \{0, 1, 2\}$ and let S be the set of all strings over A. Define a relation L from S to $\mathbf{Z}^{nonneg}$ as follows: For every string s in S and every nonnegative integer n,

$$(s, n) \in L \quad \text{means that} \quad \text{the length of } s \text{ is } n.$$

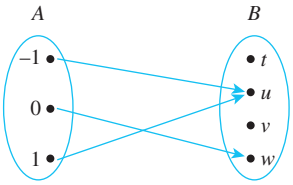
Then L is a function because every string in S has one and only one length. Find $L(0201)$ and $L(12)$.

12. Let $A = \{x, y\}$ and let S be the set of all strings over A. Define a relation C from S to S as follows: For all strings s and t in S,

$$(s, t) \in C \quad \text{means that} \quad t = ys.$$

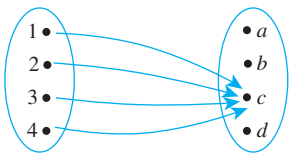
Then C is a function because every string in S consists entirely of x's and y's and adding an additional y on the left creates a single new string that consists of x's and y's and is, therefore, also in S. Find $C(x)$ and $C(yyxyx)$.

13. Let $A = \{-1, 0, 1\}$ and $B = \{t, u, v, w\}$. Define a function $F: A \to B$ by the following arrow diagram:



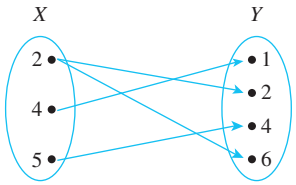
a. Write the domain and co-domain of F.
b. Find $F(-1)$, $F(0)$, and $F(1)$.

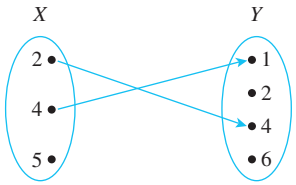
14. Let $C = \{1, 2, 3, 4\}$ and $D = \{a, b, c, d\}$. Define a function $G: C \to D$ by the following arrow diagram:

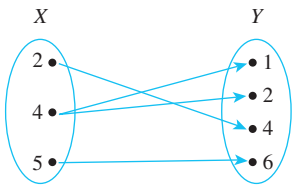


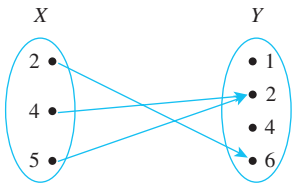
a. Write the domain and co-domain of G.
b. Find $G(1)$, $G(2)$, $G(3)$, and $G(4)$.

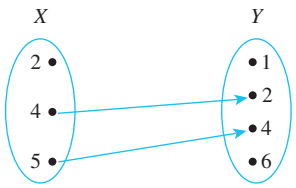
15. Let $X = \{2, 4, 5\}$ and $Y = \{1, 2, 4, 6\}$. Which of the following arrow diagrams determine functions from X to Y?

a.


b.


c.


d.


e.


16. Let f be the squaring function defined in Example 1.3.6. Find $f(-1)$, $f(0)$, and $f\left(\frac{1}{2}\right)$.

17. Let g be the successor function defined in Example 1.3.6. Find $g(-1000)$, $g(0)$, and $g(999)$.

18. Let h be the constant function defined in Example 1.3.6. Find $h\left(-\frac{12}{5}\right)$, $h\left(\frac{0}{1}\right)$, and $h\left(\frac{9}{17}\right)$.

19. Define functions f and g from $\mathbf{R}$ to $\mathbf{R}$ by the following formulas: For every $x \in \mathbf{R}$,

$$f(x) = 2x \quad \text{and} \quad g(x) = \frac{2x^3 + 2x}{x^2 + 1}.$$

Does $f = g$? Explain.

20. Define functions H and K from $\mathbf{R}$ to $\mathbf{R}$ by the following formulas: For every $x \in \mathbf{R}$,

$$H(x) = (x-2)^2 \quad \text{and} \quad K(x) = (x-1)(x-3) + 1.$$

Does $H = K$? Explain.

ANSWERS FOR TEST YOURSELF

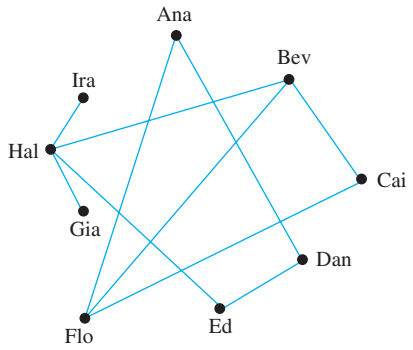
1. a subset of the Cartesian product $A \times B$ **2.** a. an element y of B such that $(x, y) \in F$ (i.e., such that x is related to y by F) b. $(x, y) \in F$ and $(x, z) \in F$; $y = z$ **3.** the unique element of B that is related to x by F

1.4 The Language of Graphs

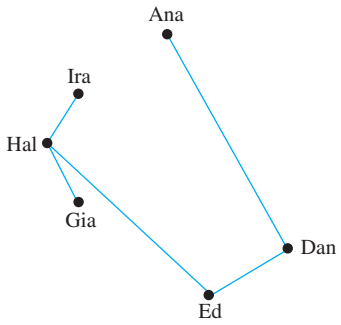
The whole of mathematics consists in the organization of a series of aids to the imagination in the process of reasoning. —Alfred North Whitehead, 1861–1947

Imagine an organization that wants to set up teams of three to work on some projects. In order to maximize the number of people on each team who had previous experience working together successfully, the director asked the members to provide names of their previous partners. This information is displayed below both in a table and in a diagram.

Name	Previous Partners
Ana	Dan, Flo
Bev	Cai, Flo, Hal
Cai	Bev, Flo
Dan	Ana, Ed
Ed	Dan, Hal
Flo	Cai, Bev, Ana
Gia	Hal
Hal	Gia, Ed, Bev, Ira
Ira	Hal



From the diagram, it is easy to see that Bev, Cai, and Flo are a group of three previous partners, and so it would be reasonable for them to form one of these teams. The drawing below shows the result when these three names are removed from the diagram.

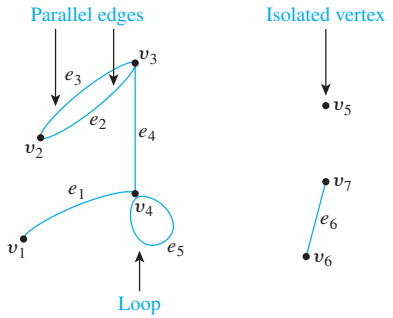


This drawing shows that placing Hal on the same team as Ed would leave Gia and Ira on a team where they would not have a previous partner. However, if Hal is placed on a team with Gia and Ira, then the remaining team would consist of Ana, Dan, and Ed, and everyone on both teams would be working with a previous partner.

Drawings such as these are illustrations of a structure known as a *graph*. The dots are called *vertices* (plural of *vertex*) and the line segments joining vertices are called *edges*. As you can see from the first drawing, it is possible for two edges to cross at a point that is not

a vertex. Note also that the type of graph described here is quite different from the "graph of an equation" or the "graph of a function."

In general, a graph consists of a set of vertices and a set of edges connecting various pairs of vertices. The edges may be straight or curved and should either connect one vertex to another or a vertex to itself, as shown below.



In this drawing, the vertices are labeled with v's and the edges with e's. When an edge connects a vertex to itself (as e_5 does), it is called a *loop*. When two edges connect the same pair of vertices (as e_2 and e_3 do), they are said to be *parallel*. It is quite possible for a vertex to be unconnected by an edge to any other vertex in the graph (as v_5 is), and in that case the vertex is said to be *isolated*. The formal definition of a graph follows.

Definition

A **graph** G consists of two finite sets: a nonempty set $V(G)$ of **vertices** and a set $E(G)$ of **edges**, where each edge is associated with a set consisting of either one or two vertices called its **endpoints**. The correspondence from edges to endpoints is called the **edge-endpoint function**.

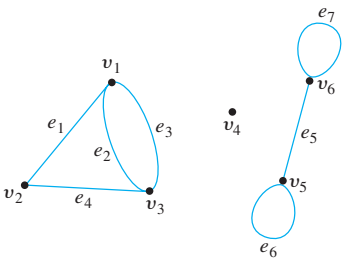
An edge with just one endpoint is called a **loop**, and two or more distinct edges with the same set of endpoints are said to be **parallel**. An edge is said to **connect** its endpoints; two vertices that are connected by an edge are called **adjacent**; and a vertex that is an endpoint of a loop is said to be **adjacent to itself**.

An edge is said to be **incident on** each of its endpoints, and two edges incident on the same endpoint are called **adjacent**. A vertex on which no edges are incident is called **isolated**.

Graphs have pictorial representations in which the vertices are represented by dots and the edges by line segments. A given pictorial representation uniquely determines a graph.

Example 1.4.1 **Terminology**

Consider the following graph:



a. Write the vertex set and the edge set, and give a table showing the edge-endpoint function.

b. Find all edges that are incident on v_1, all vertices that are adjacent to v_1, all edges that are adjacent to e_1, all loops, all parallel edges, all vertices that are adjacent to themselves, and all isolated vertices.

Solution

a. vertex set $= \{v_1, v_2, v_3, v_4, v_5, v_6\}$
edge set $= \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$
edge-endpoint function:

Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_3\}$
e_3	$\{v_1, v_3\}$
e_4	$\{v_2, v_3\}$
e_5	$\{v_5, v_6\}$
e_6	$\{v_5\}$
e_7	$\{v_6\}$

Note The isolated vertex v_4 does not appear in the table. Although each edge of a graph must have either one or two endpoints, a vertex need not be an endpoint of an edge.

b. e_1, e_2, and e_3 are incident on v_1.
v_2 and v_3 are adjacent to v_1.
e_2, e_3, and e_4 are adjacent to e_1.
e_6 and e_7 are loops.
e_2 and e_3 are parallel.
v_5 and v_6 are adjacent to themselves.
v_4 is an isolated vertex. ■

Although a given pictorial representation uniquely determines a graph, a given graph may have more than one pictorial representation. Such things as the lengths or curvatures of the edges and the relative position of the vertices on the page may vary from one pictorial representation to another.

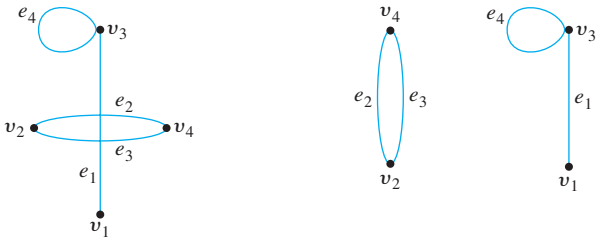
Example 1.4.2 **Drawing More Than One Picture for a Graph**

Consider the graph specified as follows:

vertex set $= \{v_1, v_2, v_3, v_4\}$
edge set $= \{e_1, e_2, e_3, e_4\}$
edge-endpoint function:

Edge	Endpoints
e_1	$\{v_1, v_3\}$
e_2	$\{v_2, v_4\}$
e_3	$\{v_2, v_4\}$
e_4	$\{v_3\}$

Both drawings (a) and (b) shown below are pictorial representations of this graph.



Example 1.4.3 **Labeling Drawings to Show They Represent the Same Graph**

Consider the two drawings shown in Figure 1.4.1. Label vertices and edges in such a way that both drawings represent the same graph.

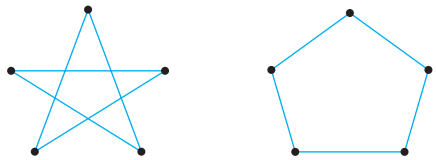
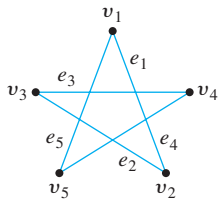
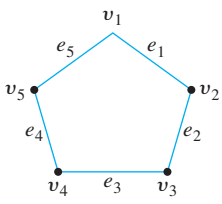


FIGURE 1.4.1

Solution Imagine putting one end of a piece of string at the top vertex of Figure 1.4.1(a) (call this vertex v_1), then laying the string to the next adjacent vertex on the lower right (call this vertex v_2), then laying it to the next adjacent vertex on the upper left (v_3), and so forth, returning finally to the top vertex v_1. Call the first edge e_1, the second e_2, and so forth, as shown below.



Now imagine picking up the piece of string, together with its labels, and repositioning it as follows:



This is the same as Figure 1.4.1(b), so both drawings represent the graph with vertex set $\{v_1, v_2, v_3, v_4, v_5\}$, edge set $\{e_1, e_2, e_3, e_4, e_5\}$, and edge-endpoint function as follows:

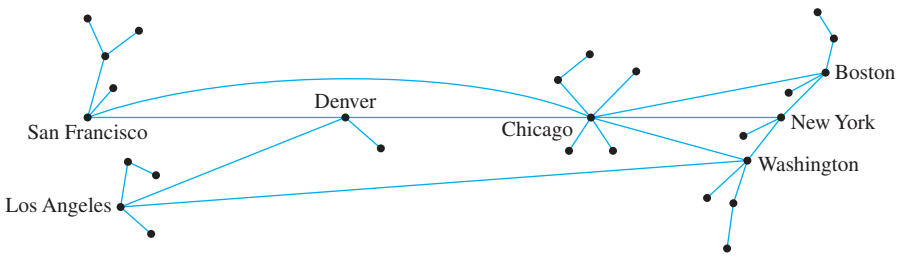
Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_3, v_4\}$
e_4	$\{v_4, v_5\}$
e_5	$\{v_5, v_1\}$

Examples of Graphs

Graphs are a powerful problem-solving tool because they enable us to represent a complex situation with a single image that can be analyzed both visually and with the aid of a computer. A few examples follow, and others are included in the exercises.

Example 1.4.4 **Using a Graph to Represent a Network**

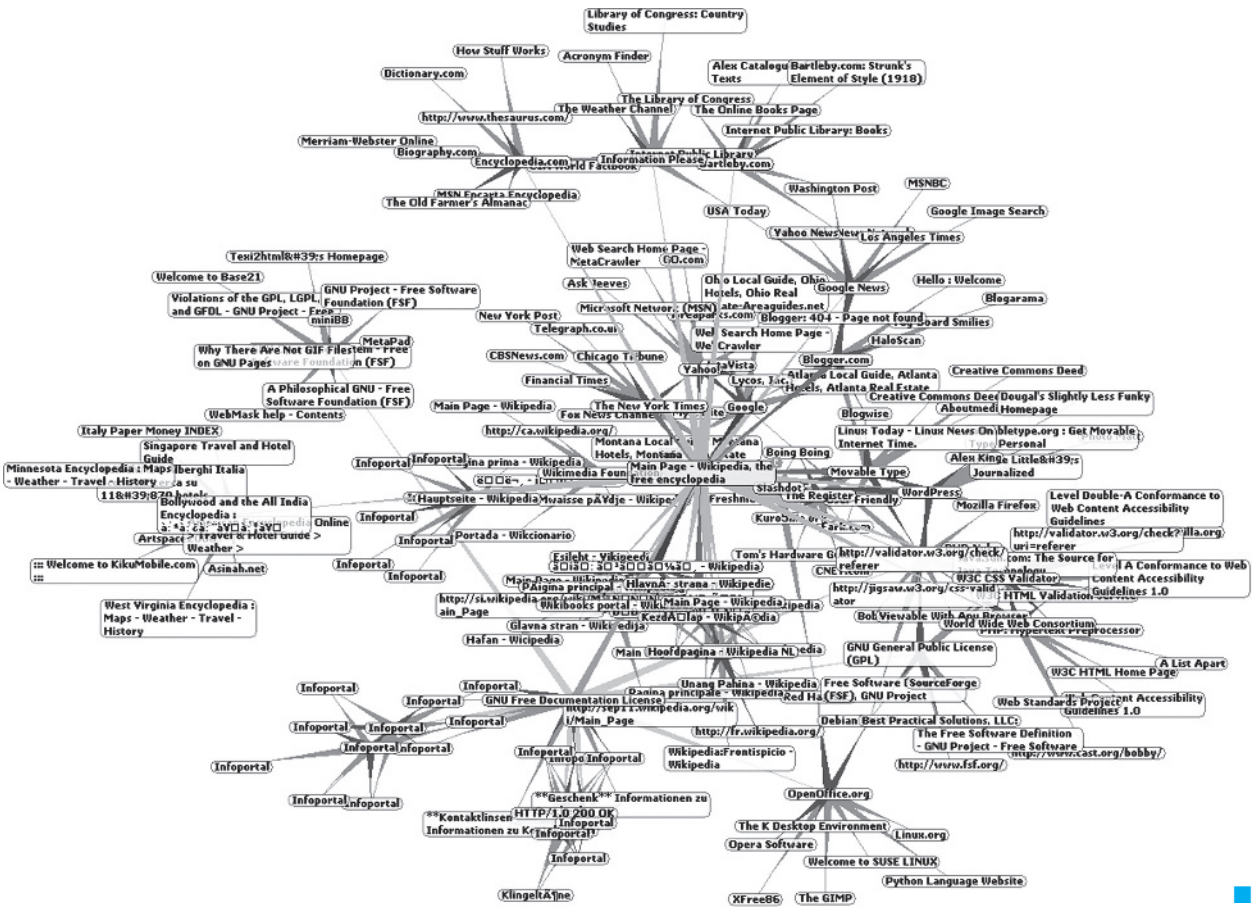
Telephone, electric power, gas pipeline, and air transport systems can all be represented by graphs, as can computer networks—from small local area networks to the global Internet system that connects millions of computers worldwide. Questions that arise in the design of such systems involve choosing connecting edges to minimize cost, optimize a certain type of service, and so forth. A typical network, called a *hub-and-spoke model*, is shown below.



Example 1.4.5 **Using a Graph to Represent the World Wide Web**

The World Wide Web, or Web, is a system of interlinked documents, or webpages, contained on the Internet. Users employing Web browsers, such as Internet Explorer, Chrome, Safari, and Firefox, can move quickly from one webpage to another by clicking on hyperlinks, which use versions of software called hypertext transfer protocols (HTTPs). Individuals and individual companies create the pages, which they transmit to servers that contain software capable of delivering them to those who request them through a Web browser. Because the amount of information currently on the Web is so vast, search engines, such as Google, Yahoo, and Bing, have algorithms for finding information very efficiently.

The following picture shows a minute fraction of the hyperlink connections on the Internet that radiate in and out from the Wikipedia main page.



A *directed graph* is like an (undirected) graph except that each edge is associated with an *ordered pair* of vertices rather than a *set* of vertices. Thus each edge of a directed graph can be drawn as an arrow going from the first vertex to the second vertex of the ordered pair.

Note Each directed graph has an associated ordinary (undirected) graph, which is obtained by ignoring the directions of the edges.

Definition

A **directed graph**, or **digraph**, consists of two finite sets: a nonempty set $V(G)$ of vertices and a set $D(G)$ of directed edges, where each is associated with an ordered pair of vertices called its **endpoints**. If edge e is associated with the pair (v, w) of vertices, then e is said to be the (**directed**) **edge** from v to w.

Example 1.4.6 **Using a Graph to Represent Knowledge**

In many applications of artificial intelligence, a knowledge base of information is collected and represented inside a computer. Because of the way the knowledge is represented and because of the properties that govern the artificial intelligence program, the computer is not limited to retrieving data in the same form as it was entered; it can also derive new facts from the knowledge base by using certain built-in rules of inference. For example, from the knowledge that the *Los Angeles Times* is a big-city daily and that a big-city daily contains national news, an artificial intelligence program could infer that the *Los Angeles Times*

contains national news. The directed graph shown in Figure 1.4.2 is a pictorial representation for a simplified knowledge base about periodical publications.

According to this knowledge base, what paper finish does the *New York Times* use?

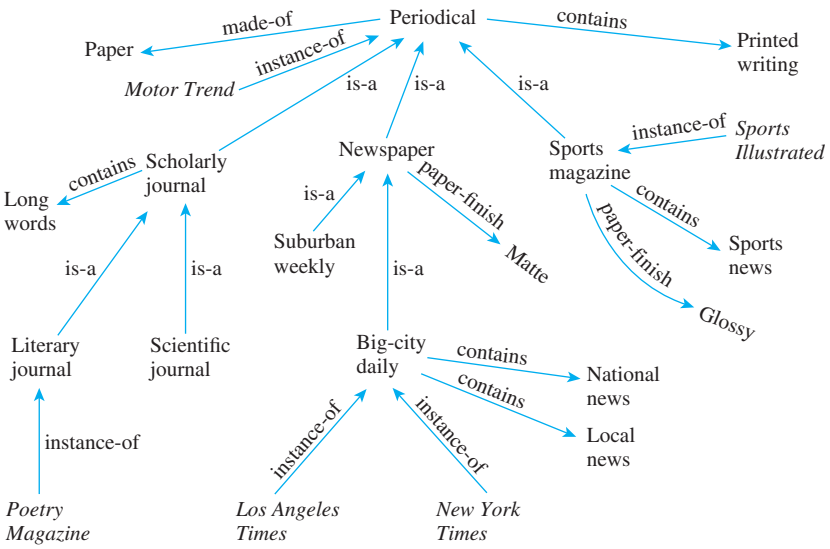


FIGURE 1.4.2

Solution The arrow going from *New York Times* to big-city daily (labeled "instance-of") shows that the *New York Times* is a big-city daily. The arrow going from big-city daily to newspaper (labeled "is-a") shows that a big-city daily is a newspaper. The arrow going from newspaper to matte (labeled "paper-finish") indicates that the paper finish on a newspaper is matte. Hence it can be inferred that the paper finish on the *New York Times* is matte. ■

Example 1.4.7 **Using a Graph to Solve a Problem: Vegetarians and Cannibals**

The following is a variation of a famous puzzle often used as an example in the study of artificial intelligence. It concerns an island on which all the people are of one of two types, either vegetarians or cannibals. Initially, two vegetarians and two cannibals are on the left bank of a river. With them is a boat that can hold a maximum of two people. The aim of the puzzle is to find a way to transport all the vegetarians and cannibals to the right bank of the river. What makes this difficult is that at no time can the number of cannibals on either bank outnumber the number of vegetarians. Otherwise, disaster befalls the vegetarians!

Solution A systematic way to approach this problem is to introduce a notation that can indicate all possible arrangements of vegetarians, cannibals, and the boat on the banks of the river. For example, you could write (*vvc* / *Bc*) to indicate that there are two vegetarians and one cannibal on the left bank and one cannibal and the boat on the right bank. Then (*vvccB* /) would indicate the initial position in which both vegetarians, both cannibals, and the boat are on the left bank of the river. The aim of the puzzle is to figure out a sequence of moves to reach the position (/ *Bvvcc*) in which both vegetarians, both cannibals, and the boat are on the right bank of the river.

Construct a graph whose vertices are the various arrangements that can be reached in a sequence of legal moves starting from the initial position. Connect vertex x to vertex y if it is possible to reach vertex y in one legal move from vertex x. For instance, from the initial

position there are four legal moves: one vegetarian and one cannibal can take the boat to the right bank; two cannibals can take the boat to the right bank; one cannibal can take the boat to the right bank; or two vegetarians can take the boat to the right bank. You can show these by drawing edges connecting vertex (*vvccB* /) to vertices (*vc* / *Bvc*), (*vv* / *Bcc*), (*vvc* / *Bc*), and (*cc* / *Bvv*). (It might seem natural to draw directed edges rather than undirected edges from one vertex to another. The rationale for drawing undirected edges is that each legal move is reversible.) From the position (*vc* / *Bvc*), the only legal moves are to go back to (*vvccB* /) or to go to (*vvcB* / *c*). You can also show these by drawing in edges. Continue this process until finally you reach (/ *Bvvcc*). From Figure 1.4.3 it is apparent that one successful sequence of moves is (*vvccB* /) ⟶ (*vc* / *Bvc*) ⟶ (*vvcB* / *c*) ⟶ (*c* / *Bvvc*) ⟶ (*ccB* / *vv*) ⟶(/ *Bvvcc*).

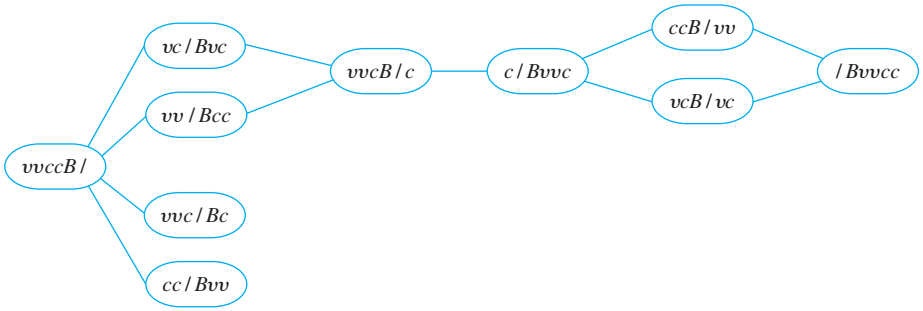
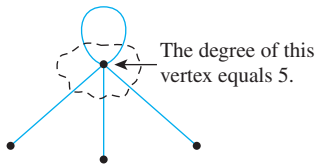


FIGURE 1.4.3 ■

Definition

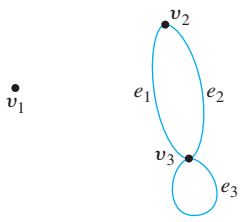
Let G be a graph and v a vertex of G. The **degree of v**, denoted **deg(v)**, equals the number of edges that are incident on v, with an edge that is a loop counted twice.

Since an edge that is a loop is counted twice, the degree of a vertex can be obtained from the drawing of a graph by counting how many end segments of edges are incident on the vertex. This is illustrated below.



Example 1.4.8 **Degree of a Vertex**

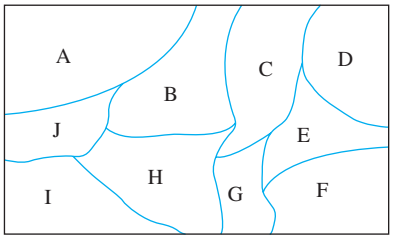
Find the degree of each vertex of the graph G shown below.



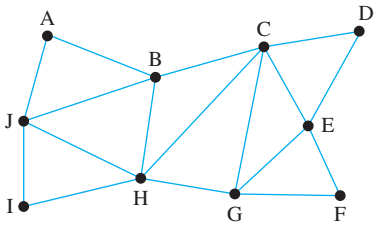
Solution $\deg(v_1) = 0$ since no edge is incident on v_1 (v_1 is isolated).
$\deg(v_2) = 2$ since both e_1 and e_2 are incident on v_2.
$\deg(v_3) = 4$ since e_1 and e_2 are incident on v_3 and the loop e_3 is also incident on v_3 (and contributes 2 to the degree of v_3). ■

Example 1.4.9 **Using a Graph to Color a Map**

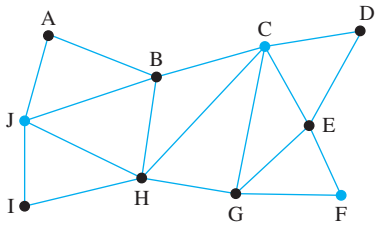
Imagine that the diagram shown below is a map with countries labeled *A*–*J*. Show that you can color the map so that no two adjacent countries have the same color.



Solution Notice that coloring the map does not depend on the sizes or shapes of the countries, but only on which countries are adjacent to which. So, to figure out a coloring, you can draw a graph, as shown below, where vertices represent countries and where edges are drawn between pairs of vertices that represent adjacent countries. Coloring the vertices of the graph will translate to coloring the countries on the map.



As you assign colors to vertices, a relatively efficient strategy is, at each stage, to focus on an uncolored vertex that has maximum degree, in other words that is connected to a maximum number of other uncolored vertices. If there is more than one such vertex, it does not matter which you choose because there are often several acceptable colorings for a given graph. For this graph, both *C* and *H* have maximum degree so you can choose one, say, *C*, and color it, say, blue. Now since *A*, *F*, *I*, and *J* are not connected to *C*, some of them may also be colored blue, and, because *J* is connected to a maximum number of others, you could start by coloring it blue. Then *F* is the only remaining vertex not connected to either *C* or *J*, so you can also color *F* blue. The drawing below shows the graph with vertices *C*, *J*, and *F* colored blue.



Since the vertices adjacent to *C*, *J*, and *F* cannot be colored blue, you can simplify the job of choosing additional colors by removing *C*, *J*, and *F* and the edges connecting them to adjacent vertices. The result is shown in Figure 1.4.4a.

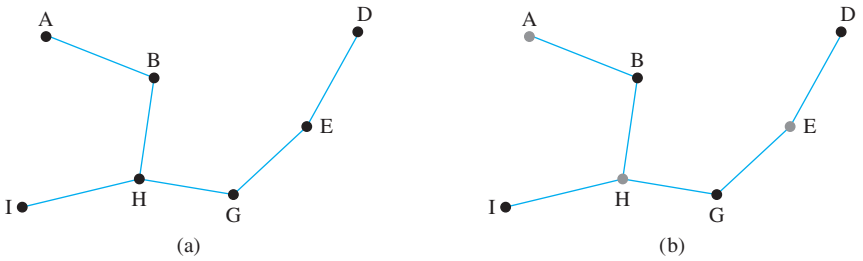
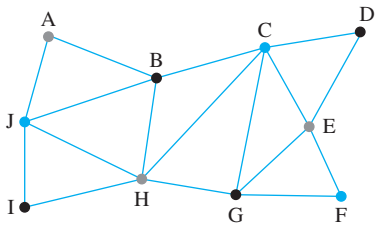
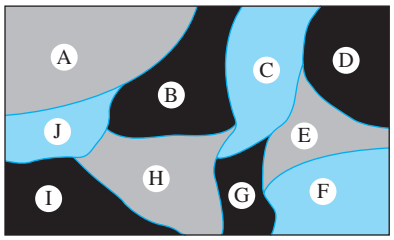


FIGURE 1.4.4

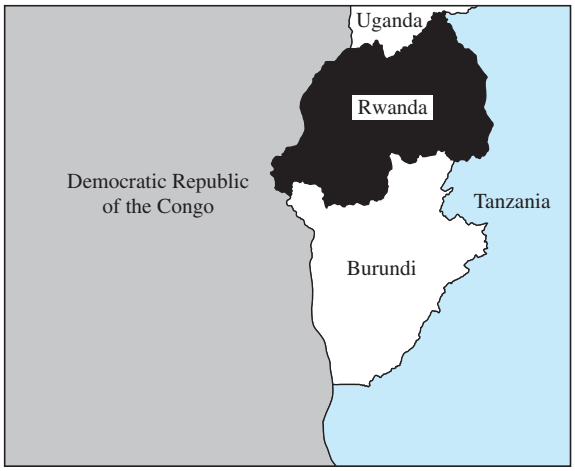
In the simplified graph again choose a vertex that has a maximum degree, namely *H*, and give it a second color, say, gray. Since *A*, *D*, and *E* are not connected to *H*, some of them may also be colored gray, and, because *E* is connected to a maximum number of these vertices, you could start by coloring *E* gray. Then *A* is not connected to *E*, and so you can also color *A* gray. This is shown in Figure 1.4.4b. The drawing below shows the original graph with vertices *C*, *J*, and *F* colored blue, vertices *H*, *A*, and *E*, colored gray, and the remaining vertices colored black. You can check that no two adjacent vertices have the same color.



Translating the graph coloring back to the original map gives the following picture in which no two adjacent countries have the same color.



The final map in Example 1.4.9 was drawn with three colors. Two colors are not enough because, for example, since *B*, *C*, and *H* are all adjacent to each other, different colors must be used for all three. The following drawing shows a map of part of Central Africa that requires four colors. Take a moment to try to assign colors to the different countries so that you see why three colors are not enough.



In the mid-1800s it was conjectured that any map, however complex, could be colored with just four colors with no two adjacent regions having the same color. The conjecture is now known as the *four-color theorem* because it was finally proved true in 1976 by Kenneth Appel and Wolfgang Haken, at the University of Illinois at Urbana-Champaign. They represented maps as graphs and used an innovative and controversial technique that combined mathematical deduction with computer examination of almost 2000 special cases.

In 1950 Edward Nelson, a university student, posed the following question: How many colors are needed to create a coloring for all the points in an ordinary (Euclidean) plane so that no two points separated by a unit distance have the same color? Nelson himself found that three colors are not enough, and a fellow student, John Isbell, developed an example showing that seven colors could be used. Thus the minimum number had to be 4, 5, or 6. Over the years a number of mathematicians tried to narrow the possibilities further, but it was not until 2018 that an English biologist and amateur mathematician, Aubrey de Grey, using a combination of ingenuity and computer calculations, created an example showing that four colors are not enough. As of the publication of this book, the complete answer to Nelson's question is still unknown, but de Grey has now proved that it must be either 5 or 6.

It turns out that a variety of problems can be modeled by representing their features with a graph and solved by finding a coloring for the vertices of the graph. For example, scheduling committee meetings when members serve on more than one committee but the meetings must be held during a fixed number of time slots or scheduling final exams for a group of courses so that no student has more than two exams on any one day. See exercises 16 and 17 at the end of this section for details about these.

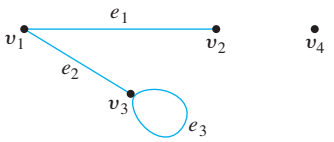
TEST YOURSELF

1. A graph consists of two finite sets: _____ and _____, where each edge is associated with a set consisting of _____.
2. A loop in a graph is _____.
3. Two distinct edges in a graph are parallel if, and only if, _____.
4. Two vertices are called adjacent if, and only if, _____.
5. An edge is incident on _____.
6. Two edges incident on the same endpoint are _____.
7. A vertex on which no edges are incident is _____.
8. In a directed graph, each edge is associated with _____.
9. The degree of a vertex in a graph is ____.

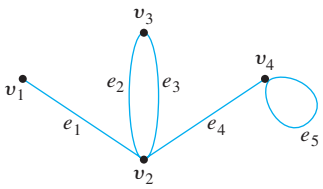
EXERCISE SET 1.4

In 1 and 2, graphs are represented by drawings. Define each graph formally by specifying its vertex set, its edge set, and a table giving the edge-endpoint function.

1.



2.



In 3 and 4, draw pictures of the specified graphs.

3. Graph G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and edge set $\{e_1, e_2, e_3, e_4\}$, with edge-endpoint function as follows:

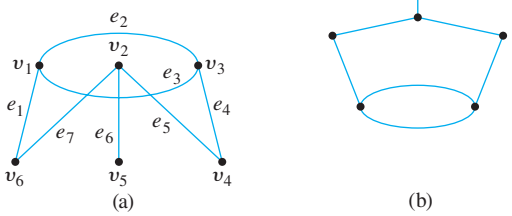
Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_2\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_2\}$

4. Graph H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and edge set $\{e_1, e_2, e_3, e_4\}$ with edge-endpoint function as follows:

Edge	Endpoints
e_1	$\{v_1\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_1, v_5\}$

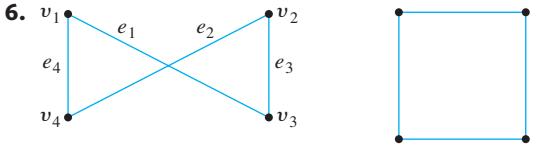
In 5–7, show that the two drawings represent the same graph by labeling the vertices and edges of the right-hand drawing to correspond to those of the left-hand drawing.

5.



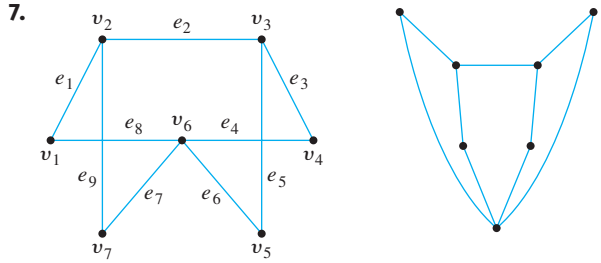
(a) (b)

6.



(a) (b)

7.

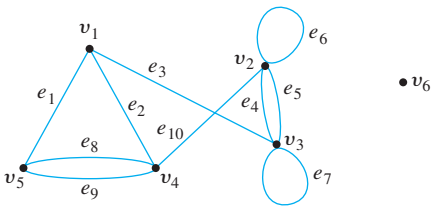


(a) (b)

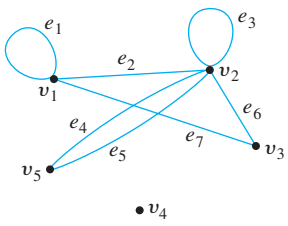
For each of the graphs in 8 and 9:

(i) Find all edges that are incident on v_1.
(ii) Find all vertices that are adjacent to v_3.
(iii) Find all edges that are adjacent to e_1.
(iv) Find all loops.
(v) Find all parallel edges.
(vi) Find all isolated vertices.
(vii) Find the degree of v_3.

8.



9.



10. Use the graph of Example 1.4.6 to determine
a. whether *Sports Illustrated* contains printed writing;
b. whether *Poetry Magazine* contains long words.

11. Find three other winning sequences of moves for the vegetarians and the cannibals in Example 1.4.7.

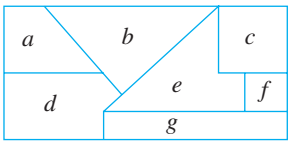
12. Another famous puzzle used as an example in the study of artificial intelligence seems first to have

appeared in a collection of problems, *Problems for the Quickening of the Mind*, which was compiled about A.D. 775. It involves a wolf, a goat, a bag of cabbage, and a ferryman. From an initial position on the left bank of a river, the ferryman is to transport the wolf, the goat, and the cabbage to the right bank. The difficulty is that the ferryman's boat is only big enough for him to transport one object at a time, other than himself. Yet, for obvious reasons, the wolf cannot be left alone with the goat, and the goat cannot be left alone with the cabbage. How should the ferryman proceed?

13. Solve the vegetarians-and-cannibals puzzle for the case where there are three vegetarians and three cannibals to be transported from one side of a river to the other.

***H* 14.** Two jugs A and B have capacities of 3 quarts and 5 quarts, respectively. Can you use the jugs to measure out exactly 1 quart of water, while obeying the following restrictions? You may fill either jug to capacity from a water tap; you may empty the contents of either jug into a drain; and you may pour water from either jug into the other.

15. Imagine that the diagram shown below is a map with countries labeled a–g. Is it possible to color the map with only three colors so that no two adjacent countries have the same color? To answer this question, follow the procedure suggested by Example 1.4.9. Draw and analyze a graph in which each country is represented by a vertex and two vertices are connected by an edge if, and only if, the countries share a common border.



***H* 16.** In this exercise a graph is used to help solve a scheduling problem. Twelve faculty members in a mathematics department serve on the following committees:

Undergraduate Education: Tenner, Peterson, Kashina, Degras

Graduate Education: Hu, Ramsey, Degras, Bergen

Colloquium: Carroll, Drupieski, Au-Yeung

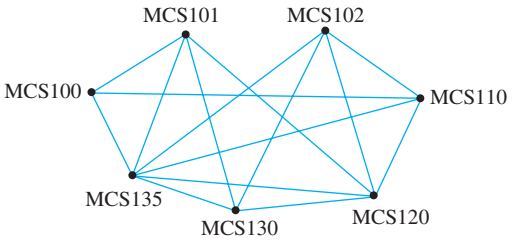
Library: Ugarcovici, Tenner, Carroll

Hiring: Hu, Drupieski, Ramsey, Peterson

Personnel: Ramsey, Wang, Ugarcovici

The committees must all meet during the first week of classes, but there are only three time slots available. Find a schedule that will allow all faculty members to attend the meetings of all committees on which they serve. To do this, represent each committee as the vertex of a graph, and draw an edge between two vertices if the two committees have a common member. Find a way to color the vertices using only three colors so that no two committees have the same color, and explain how to use the result to schedule the meetings.

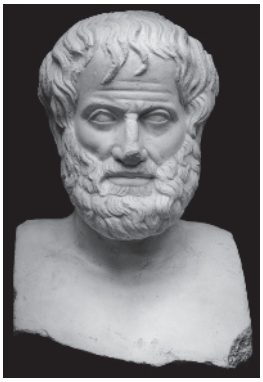
17. A department wants to schedule final exams so that no student has more than one exam on any given day. The vertices of the graph below show the courses that are being taken by more than one student, with an edge connecting two vertices if there is a student in both courses. Find a way to color the vertices of the graph with only four colors so that no two adjacent vertices have the same color and explain how to use the result to schedule the final exams.



ANSWERS FOR TEST YOURSELF

1. a finite, nonempty set of vertices; a finite set of edges; one or two vertices called its endpoints **2.** an edge with a single endpoint **3.** they have the same set of endpoints **4.** they are connected by an edge **5.** each of its endpoints **6.** adjacent **7.** isolated **8.** an ordered pair of vertices called its endpoints **9.** the number of edges that are incident on the vertex, with an edge that is a loop counted twice

CHAPTER 2 THE LOGIC OF COMPOUND STATEMENTS



Mohamed Osama/Alamy Stock Photo

Aristotle
(384 B.C.–322 B.C.)

The first great treatises on logic were written by the Greek philosopher Aristotle. They were a collection of rules for deductive reasoning that were intended to serve as a basis for the study of every branch of knowledge. In the seventeenth century, the German philosopher and mathematician Gottfried Leibniz conceived the idea of using symbols to mechanize the process of deductive reasoning in much the same way that algebraic notation had mechanized the process of reasoning about numbers and their relationships. Leibniz's idea was realized in the nineteenth century by the English mathematicians George Boole and Augustus De Morgan, who founded the modern subject of symbolic logic. With research continuing to the present day, symbolic logic has provided, among other things, the theoretical basis for many areas of computer science such as digital logic circuit design (see Sections 2.4 and 2.5), relational database theory (see Section 8.1), automata theory and computability (see Section 7.4 and Chapter 12), and artificial intelligence (see Sections 3.3, 10.1, and 10.5).

2.1 Logical Form and Logical Equivalence

Logic is a science of the necessary laws of thought, without which no employment of the understanding and the reason takes place. —Immanuel Kant, 1785

An argument is a sequence of statements aimed at demonstrating the truth of an assertion. The assertion at the end of the sequence is called the *conclusion*, and the preceding statements are called *premises*. To have confidence in the conclusion that you draw from an argument, you must be sure that the premises are acceptable on their own merits or follow from other statements that are known to be true.

In logic, the form of an argument is distinguished from its content. Logical analysis won't help you determine the intrinsic merit of an argument's content, but it will help you analyze an argument's form to determine whether the truth of the conclusion follows *necessarily* from the truth of the premises. For this reason logic is sometimes defined as the science of necessary inference or the science of reasoning.

Consider the following two arguments. They have very different content but their logical form is the same. To help make this clear, we use letters like p, q, and r to represent component sentences; we let the expression "not p" refer to the sentence "It is not the case that p"; and we let the symbol $\therefore$ stand for the word "therefore."

Argument 1

$$\overbrace{\text{If the bell rings}}^{p} \text{ or } \overbrace{\text{the flag drops}}^{q}, \text{ then } \overbrace{\text{the race is over}}^{r}.$$

$$\therefore \overbrace{\text{If the race is not over}}^{\text{not } r}, \text{ then } \overbrace{\text{the bell hasn't rung}}^{\text{not } p} \text{ and } \overbrace{\text{the flag hasn't dropped}}^{\text{not } q}.$$

Argument 2

$$\text{If } \overbrace{x = 2}^{p} \text{ or } \overbrace{x = -2}^{q}, \text{ then } \overbrace{x^2 = 4}^{r}.$$
$$\therefore \text{If } \overbrace{x^2 \neq 4}^{\text{not } r}, \text{ then } \overbrace{x \neq 2}^{\text{not } p} \text{ and } \overbrace{x \neq -2}^{\text{not } q}.$$

The common form of the arguments is

If p or q, then r.
$\therefore$ If not r, then not p and not q.

In exercise 10 in Section 2.3 you will show that this form of argument is *valid* in the sense that *if* its assumptions are true, then its conclusion must also be true.

Example 2.1.1 **Identifying Logical Form**

Fill in the blanks below so that argument (b) has the same form as argument (a). Then represent the common form of the arguments using letters to stand for component sentences.

a. If Jane is a math major or Jane is a computer science major, then Jane will take Math 150.
Jane is a computer science major.
Therefore, Jane will take Math 150.

b. If logic is easy or ___(1)___, then ___(2)___.
I will study hard.
Therefore, I will get an A in this course.

Solution

1. I (will) study hard.
2. I will get an A in this course.

Common form: If p or q, then r.
q.
Therefore, r. ■

Statements

Most of the definitions of formal logic have been developed so that they agree with the natural or intuitive logic used by people who have been educated to think clearly and use language carefully. The differences that exist between formal and intuitive logic are necessary to avoid ambiguity and obtain consistency.

In any mathematical theory, new terms are defined by using those that have been previously defined. However, this process has to start somewhere. A few initial terms necessarily remain undefined. In logic, the words *sentence*, *true*, and *false* are the initial undefined terms.

Definition

A **statement** (or **proposition**) is a sentence that is true or false but not both.

For example, "Two plus two equals four" and "Two plus two equals five" are both statements, the first because it is true and the second because it is false. On the other hand, the truth or falsity of

$$x^2 + 2 = 11$$

depends on the value of x. For some values of x, it is true ($x = 3$ and $x = -3$), whereas for other values it is false. Similarly, the truth or falsity of

$$x + y > 0$$

depends on the values of x and y. For instance, when $x = -1$ and $y = 2$ it is true, whereas when $x = -1$ and $y = 1$ it is false. In Section 3.1 we will discuss ways to transform sentences of these forms into statements.

Compound Statements

We now introduce three symbols that are used to build more complicated logical expressions out of simpler ones. The symbol $\sim$ denotes *not*, $\wedge$ denotes *and*, and $\vee$ denotes *or*. Given a statement p, the sentence "$\sim p$" is read "not p" or "It is not the case that p." In some computer languages the symbol $\neg$ is used in place of $\sim$. Given another statement q, the sentence "$p \wedge q$" is read "p and q." The sentence "$p \vee q$" is read "p or q."

Note $\sim p$ means "not p"
$p \wedge q$ means "p and q"
$p \vee q$ means "p or q"

In expressions that include the symbol $\sim$ as well as $\wedge$ or $\vee$, the **order of operations** specifies that $\sim$ is performed first. For instance, $\sim p \wedge q = (\sim p) \wedge q$. In logical expressions, as in ordinary algebraic expressions, the order of operations can be overridden through the use of parentheses. Thus $\sim(p \wedge q)$ represents the negation of the conjunction of p and q. In this, as in most treatments of logic, the symbols $\wedge$ and $\vee$ are considered coequal in order of operation, and an expression such as $p \wedge q \vee r$ is considered ambiguous. This expression must be written as either $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$ to have meaning.

A variety of English words translate into logic as $\wedge$, $\vee$, or $\sim$. For instance, the word *but* translates the same as *and* when it links two independent clauses, as in "Jim is tall but he is not heavy." Generally, the word *but* is used in place of *and* when the part of the sentence that follows is, in some way, unexpected. Another example involves the words *neither-nor*. When Shakespeare wrote, "Neither a borrower nor a lender be," he meant, "Do not be a borrower and do not be a lender." So if p and q are statements, then

p but q	means	p and q
neither p nor q	means	$\sim p$ and $\sim q$.

Example 2.1.2 **Translating from English to Symbols: *But* and *Neither-Nor***

Write each of the following sentences symbolically, letting h = "It is hot" and s = "It is sunny."

a. It is not hot but it is sunny.

b. It is neither hot nor sunny.

Solution

a. The given sentence is equivalent to "It is not hot and it is sunny," which can be written symbolically as $\sim h \wedge s$.

b. To say it is neither hot nor sunny means that it is not hot and it is not sunny. Therefore, the given sentence can be written symbolically as $\sim h \wedge \sim s$. ■

The notation for inequalities involves *and* and *or* statements. For instance, if x, a, and b are particular real numbers, then

$x \le a$	means	$x < a$	or	$x = a$
$a \le x \le b$	means	$a \le x$	and	$x \le b$.

Note The point of specifying x, a, and b to be *particular* real numbers is to ensure that sentences such as "$x < a$" and "$x \ge b$" are either true or false and hence that they are statements.

Note that the inequality $2 \le x \le 1$ is not satisfied by any real numbers because

$2 \le x \le 1$	means	$2 \le x$	and	$x \le 1$,

and this is false no matter what number x happens to be.

Example 2.1.3 ***And*, *Or*, and Inequalities**

Suppose x is a particular real number. Let p, q, and r symbolize "$0 < x$," "$x < 3$," and "$x = 3$," respectively. Write the following inequalities symbolically:

a. $x \le 3$ b. $0 < x < 3$ c. $0 < x \le 3$

Solution

a. $q \vee r$ b. $p \wedge q$ c. $p \wedge (q \vee r)$ ■

Truth Values

In Examples 2.1.2 and 2.1.3 we built compound sentences out of component statements and the terms *not*, *and*, and *or*. If such sentences are to be statements, however, they must have well-defined **truth values**—they must be either true or false. We now define such compound sentences as statements by specifying their truth values in terms of the statements that compose them.

Note Think of negation like this:
The negation of a statement is a statement that exactly expresses what it would mean for the statement to be false.

Definition

If p is a statement variable, the **negation** of p is "not p" or "It is not the case that p" and is denoted $\sim p$. It has opposite truth value from p: if p is true, $\sim p$ is false; if p is false, $\sim p$ is true.

The truth values for negation are summarized in a *truth table*.

Truth Table for $\sim p$

p	$\sim p$
T	F
F	T

In ordinary language the sentence "It is hot and it is sunny" is understood to be true when both conditions—being hot and being sunny—are satisfied. If it is hot but not sunny, or sunny but not hot, or neither hot nor sunny, the sentence is understood to be

false. The formal definition of truth values for an *and* statement agrees with this general understanding.

Definition

If p and q are statement variables, the **conjunction** of p and q is "p and q," denoted $p \wedge q$. It is true when, and only when, both p and q are true. If either p or q is false, or if both are false, $p \wedge q$ is false.

The truth values for conjunction can also be summarized in a truth table. The table is obtained by considering the four possible combinations of truth values for p and q. Each combination is displayed in one row of the table; the corresponding truth value for the whole statement is placed in the right-most column of that row. Note that the only row containing a T is the first one because an *and* statement is true only when both components are true.

Note The only way for an *and* statement to be true is for both components to be true. So in the truth table for an *and* statement the first row is the only row with a *T*.

Truth Table for $p \wedge q$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

The order of truth values for p and q in the table above is TT, TF, FT, FF. It is not absolutely necessary to write the truth values in this order, although it is customary to do so. So please use this order for all truth tables involving two statement variables. Example 2.1.5 shows the standard order for truth tables that involve three statement variables.

In the case of disjunction—statements of the form "p or q"—intuitive logic offers two alternative interpretations. In ordinary language *or* is sometimes used in an exclusive sense (p or q but not both) and sometimes in an inclusive sense (p or q or both). A waiter who says you may have "coffee, tea, or milk" uses the word *or* in an exclusive sense: Extra payment is generally required if you want more than one beverage. On the other hand, a waiter who offers "cream or sugar" uses the word *or* in an inclusive sense: You are entitled to both cream and sugar if you wish to have them.

Mathematicians and logicians avoid possible ambiguity about the meaning of the word *or* by understanding it to mean the inclusive "and/or." The symbol $\vee$ comes from the Latin word *vel*, which means *or* in its inclusive sense. To express the exclusive *or*, the phrase *p or q but not both* is used.

Note The statement "$2 \leq 2$" means that 2 is less than 2 or 2 equals 2. It is true because $2 = 2$.

Definition

If p and q are statement variables, the **disjunction** of p and q is "p or q," denoted $p \vee q$. It is true when either p is true, or q is true, or both p and q are true; it is false only when both p and q are false.

Here is the truth table for disjunction:

Note The only way for an *or* statement to be false is for both components to be false. So in the truth table for an *or* statement the last row is the only row with an *F*.

Truth Table for $p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Evaluating the Truth of More General Compound Statements

Note Java, C, and C++ use the following notations:

$\sim$	!
$\wedge$	&&
$\vee$	||

Now that truth values have been assigned to $\sim p$, $p \wedge q$, and $p \vee q$, consider the question of assigning truth values to more complicated expressions such as $\sim p \vee q$, $(p \vee q) \wedge \sim(p \wedge q)$, and $(p \wedge q) \vee r$. Such expressions are called *statement forms* (or *propositional forms*). The close relationship between statement forms and *Boolean expressions* is discussed in Section 2.4.

Definition

A **statement form** (or **propositional form**) is an expression made up of statement variables (such as p, q, and r) and logical connectives (such as $\sim$, $\wedge$, and $\vee$) that becomes a statement when actual statements are substituted for the component statement variables. The **truth table** for a given statement form displays the truth values that correspond to all possible combinations of truth values for its component statement variables.

To compute the truth values for a statement form, follow rules similar to those used to evaluate algebraic expressions. For each combination of truth values for the statement variables, first evaluate the expressions within the innermost parentheses, then evaluate the expressions within the next innermost set of parentheses, and so forth, until you have the truth values for the complete expression.

Example 2.1.4 **Truth Table for *Exclusive Or***

Note Exclusive *or* is often symbolized as $p \oplus q$ or p XOR q.

Construct the truth table for the statement form $(p \vee q) \wedge \sim(p \wedge q)$. Note that when *or* is used in its exclusive sense, the statement "p or q" means "p or q but not both" or "p or q and not both p and q," which translates into symbols as $(p \vee q) \wedge \sim(p \wedge q)$.

Solution Set up columns labeled p, q, $p \vee q$, $p \wedge q$, $\sim(p \wedge q)$, and $(p \vee q) \wedge \sim(p \wedge q)$. Fill in the p and q columns with all the logically possible combinations of T's and F's. Then use the truth tables for $\vee$ and $\wedge$ to fill in the $p \vee q$ and $p \wedge q$ columns with the appropriate truth values. Next fill in the $\sim(p \wedge q)$ column by taking the opposites of the truth values for $p \wedge q$. For example, the entry for $\sim(p \wedge q)$ in the first row is F because in the first row the truth value of $p \wedge q$ is T. Finally, fill in the $(p \vee q) \wedge \sim(p \wedge q)$ column by considering the truth values for an *and* statement together with the truth values for $p \vee q$ and $\sim(p \wedge q)$. Since an *and* statement is true only when both components are true and since rows 2 and 3 are the only two rows where both $p \vee q$ and $\sim(p \wedge q)$ are true, put T in rows 2 and 3 and F in the remaining rows.

Note To fill out a truth table for an *and* statement, first put a T in each row where both components are true; then put an F in each of the remaining rows.

Truth Table for *Exclusive Or:* $(p \vee q) \wedge \sim(p \wedge q)$

p	q	$p \vee q$	$p \wedge q$	$\sim(p \wedge q)$	$(p \vee q) \wedge \sim(p \wedge q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

■

Example 2.1.5 **Truth Table for $(p \wedge q) \vee \sim r$**

Note To fill out a truth table for an *or* statement, first put an F in each row where both components are false; then put a T in each of the remaining rows.

Construct a truth table for the statement form $(p \wedge q) \vee \sim r$.

Solution Make columns headed p, q, r, $p \wedge q$, $\sim r$, and $(p \wedge q) \vee \sim r$. Enter the eight logically possible combinations of truth values for p, q, and r in the three left-most columns. Then fill in the truth values for $p \wedge q$ and for $\sim r$. Complete the table by considering the truth values for $(p \wedge q)$ and for $\sim r$ and the definition of an *or* statement. Since an *or* statement is false only when both components are false, the only rows in which the entry is F are the third, fifth, and seventh rows because those are the only rows in which the expressions $p \wedge q$ and $\sim r$ are both false. The entry for all the other rows is T.

p	q	r	$p \wedge q$	$\sim r$	$(p \wedge q) \vee \sim r$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	F	T	T
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

■

The essential point about assigning truth values to compound statements is that it allows you—using logic alone—to judge the truth of a compound statement on the basis of your knowledge of the truth of its component parts. Logic does not help you determine the truth or falsity of the component statements. Rather, logic helps link these separate pieces of information together into a coherent whole.

Logical Equivalence

The statements

6 is greater than 2 and 2 is less than 6

are two different ways of saying the same thing. Why? Because of the definition of the phrases *greater than* and *less than*. By contrast, although the statements

(1) Dogs bark and cats meow and (2) Cats meow and dogs bark

are also two different ways of saying the same thing, the reason has nothing to do with the definition of the words. It has to do with the logical form of the statements. Any two statements whose logical forms are related in the same way as (1) and (2) would either both be true or both be false. You can see this by examining the following truth table, where the statement variables p and q are substituted for the component statements "Dogs bark" and "Cats meow," respectively. The table shows that for each combination of truth values for p and q, $p \wedge q$ is true when, and only when, $q \wedge p$ is true. In such a case, the statement forms are called *logically equivalent*, and we say that (1) and (2) are *logically equivalent statements.*

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

$p \wedge q$ and $q \wedge p$ always have the same truth values, so they are logically equivalent

Definition

Two *statement forms* are called **logically equivalent** if, and only if, they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted by writing $P \equiv Q$.

Two *statements* are called **logically equivalent** if, and only if, they have logically equivalent forms when identical component statement variables are used to replace identical component statements.

Testing Whether Two Statement Forms *P* and *Q* Are Logically Equivalent

1. Construct a truth table with one column for the truth values of P and another column for the truth values of Q.
2. Check each combination of truth values of the statement variables to see whether the truth value of P is the same as the truth value of Q.
   a. If in each row the truth value of P is the same as the truth value of Q, then P and Q are logically equivalent.
   b. If in some row P has a different truth value from Q, then P and Q are not logically equivalent.

Example 2.1.6 **Double Negative Property: $\sim(\sim p) \equiv p$**

Construct a truth table to show that the negation of the negation of a statement is logically equivalent to the statement, annotating the table with a sentence of explanation.

Solution

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

p and $\sim(\sim p)$ always have the same truth values, so they are logically equivalent

■

There are two ways to show that statement forms P and Q are *not* logically equivalent. As indicated previously, one is to use a truth table to find rows for which their truth values differ. The other way is to find concrete statements for each of the two forms, one of which is true and the other of which is false. The next example illustrates both of these ways.

Example 2.1.7 **Showing Nonequivalence**

Show that the statement forms $\sim(p \wedge q)$ and $\sim p \wedge \sim q$ are not logically equivalent.

Solution

a. This method uses a truth table annotated with a sentence of explanation.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$		$\sim p \wedge \sim q$
T	T	F	F	T	F		F
T	F	F	T	F	T	$\neq$	F
F	T	T	F	F	T	$\neq$	F
F	F	T	T	F	T		T

$\sim(p \wedge q)$ and $\sim p \wedge \sim q$ have different truth values in rows 2 and 3, so they are not logically equivalent

b. This method uses an example to show that $\sim(p \wedge q)$ and $\sim p \wedge \sim q$ are not logically equivalent. Let p be the statement "$0 < 1$" and let q be the statement "$1 < 0$." Then

$$\sim(p \wedge q) \quad \text{is} \quad \text{"It is not the case that both } 0 < 1 \text{ and } 1 < 0\text{,"}$$

which is true. On the other hand,

$$\sim p \wedge \sim q \quad \text{is} \quad \text{"}0 \not< 1 \quad \text{and} \quad 1 \not< 0\text{,"}$$

which is false. This example shows that there are concrete statements you can substitute for p and q to make one of the statement forms true and the other false. Therefore, the statement forms are not logically equivalent. ■

Example 2.1.8 **Negations of *And* and *Or*: De Morgan's Laws**

For the statement "John is tall and Jim is redheaded" to be true, both components must be true. So for the statement to be false, one or both components must be false. Thus the negation can be written as "John is not tall or Jim is not redheaded." In general, the negation

of the conjunction of two statements is logically equivalent to the disjunction of their negations. That is, statements of the forms $\sim(p \wedge q)$ and $\sim p \vee \sim q$ are logically equivalent. Check this using truth tables.

Solution

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$	$\sim p \vee \sim q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

$\sim(p \wedge q)$ and $\sim p \vee \sim q$ always have the same truth values, so they are logically equivalent

Symbolically,

$$\sim(p \wedge q) \equiv \sim p \vee \sim q.$$

Paul Fearn/Alamy Stock Photo

Augustus De Morgan (1806–1871)

In the exercises at the end of this section you are asked to show the analogous law that the negation of the disjunction of two statements is logically equivalent to the conjunction of their negations:

$$\sim(p \vee q) \equiv \sim p \wedge \sim q.$$

■

The two logical equivalences of Example 2.1.8 are known as **De Morgan's laws** of logic in honor of Augustus De Morgan, who was the first to state them in formal mathematical terms.

De Morgan's Laws

The negation of an *and* statement is logically equivalent to the *or* statement in which each component is negated.

The negation of an *or* statement is logically equivalent to the *and* statement in which each component is negated.

Example 2.1.9 **Applying De Morgan's Laws**

Write negations for each of the following statements:

a. John is 6 feet tall and he weighs at least 200 pounds.

b. The bus was late or Tom's watch was slow.

Solution

a. John is not 6 feet tall or he weighs less than 200 pounds.

b. The bus was not late and Tom's watch was not slow.

Since the statement "neither p nor q" means the same as "$\sim p$ and $\sim q$," an alternative answer for (b) is "Neither was the bus late nor was Tom's watch slow." ■

If x is a particular real number, saying that x is not less than 2 ($x \not< 2$) means that x does not lie to the left of 2 on the number line. This is equivalent to saying that either $x = 2$ or x lies to the right of 2 on the number line ($x = 2$ or $x > 2$). Hence,

$$x \not< 2 \quad \text{is equivalent to} \quad x \geq 2.$$

Pictorially,

If $x \not< 2$, then x lies in the shaded region.

Similarly,

$$x \not> 2 \quad \text{is equivalent to} \quad x \leq 2,$$
$$x \not\leq 2 \quad \text{is equivalent to} \quad x > 2, \text{ and}$$
$$x \not\geq 2 \quad \text{is equivalent to} \quad x < 2.$$

Example 2.1.10 **Inequalities and De Morgan's Laws**

Use De Morgan's laws to write the negation of $-1 < x \leq 4$.

Solution The given statement is equivalent to

$$-1 < x \quad \text{and} \quad x \leq 4.$$

By De Morgan's laws, the negation is

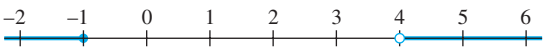
$$-1 \not< x \quad \text{or} \quad x \not\leq 4,$$

which is equivalent to

$$-1 \geq x \quad \text{or} \quad x > 4.$$

Caution! The negation of $-1 < x \leq 4$ is *not* $-1 \not< x \not\leq 4$. It is also not $-1 \geq x > 4$.

Pictorially, if $-1 \geq x$ or $x > 4$, then x lies in the shaded region of the number line, as shown below.



■

De Morgan's laws are frequently used in writing computer programs. For instance, suppose you want your program to delete all files modified outside a certain range of dates, say from date 1 through date 2 inclusive. You would use the fact that

$$\sim(date1 \leq file\_modification\_date \leq date2)$$

is equivalent to

$$(file\_modification\_date < date1) \quad \text{or} \quad (date2 < file\_modification\_date).$$

Example 2.1.11 **A Cautionary Example**

According to De Morgan's laws, the negation of

p: Jim is tall and Jim is thin

is

$\sim p$: Jim is not tall or Jim is not thin

because the negation of an *and* statement is the *or* statement in which the two components are negated.

Unfortunately, a potentially confusing aspect of the English language can arise when you are taking negations of this kind. Note that statement p can be written more compactly as

$$p'\text{: Jim is tall and thin.}$$

When it is so written, another way to negate it is

$$\sim(p')\text{: Jim is not tall and thin.}$$

Caution! Although the laws of logic are extremely useful, they should be used as an *aid* to thinking, not as a mechanical substitute for it.

But in this form the negation looks like an *and* statement. Doesn't that violate De Morgan's laws?

Actually no violation occurs. The reason is that in formal logic the words *and* and *or* are allowed only between complete statements, not between sentence fragments. So when you apply De Morgan's laws, you must have complete statements on either side of each *and* and on either side of each *or*. ■

Tautologies and Contradictions

It has been said that all of mathematics reduces to tautologies. Although this is formally true, most working mathematicians think of their subject as having substance as well as form. Nonetheless, an intuitive grasp of basic logical tautologies is part of the equipment of anyone who reasons with mathematics.

Definition

A **tautology** is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement**.

A **contradication** is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradiction is a **contradictory statement**.

According to this definition, the truth of a tautological statement and the falsity of a contradictory statement are due to the logical structure of the statements themselves and are independent of the meanings of the statements.

Example 2.1.12 **Tautologies and Contradictions**

Show that the statement form $p \vee \sim p$ is a tautology and that the statement form $p \wedge \sim p$ is a contradiction.

Solution

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
F	T	T	F
		↑ all T's, so $p \vee \sim p$ is a tautology	↑ all F's, so $p \wedge \sim p$ is a contradiction

■

Example 2.1.13 **Logical Equivalence Involving Tautologies and Contradictions**

If **t** is a tautology and **c** is a contradiction, show that $p \wedge \mathbf{t} \equiv p$ and $p \wedge \mathbf{c} \equiv \mathbf{c}$.

Solution

p	t	$p \wedge$ t	p	c	$p \wedge$ c
T	T	T	T	F	F
F	T	F	F	F	F

same truth values, so $p \wedge \mathbf{t} \equiv p$

same truth values, so $p \wedge \mathbf{c} \equiv \mathbf{c}$

■

Summary of Logical Equivalences

Knowledge of logically equivalent statements is very useful for constructing arguments. It often happens that it is difficult to see how a conclusion follows from one form of a statement, whereas it is easy to see how it follows from a logically equivalent form of the statement. A number of logical equivalences are summarized in Theorem 2.1.1 for future reference.

Theorem 2.1.1 Logical Equivalences

Given any statement variables p, q, and r, a tautology **t** and a contradiction **c**, the following logical equivalences hold.

1.	*Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2.	*Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3.	*Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4.	*Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5.	*Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6.	*Double negative law:*	$\sim(\sim p) \equiv p$	
7.	*Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8.	*Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9.	*De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10.	*Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11.	*Negations of* **t** *and* **c**:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

The proofs of laws 4 and 6, the first parts of laws 1 and 5, and the second part of law 9 have already been given as examples in the text. Proofs of the other parts of the theorem are left as exercises. In fact, it can be shown that the first five laws of Theorem 2.1.1 form a core from which the other laws can be derived. The first five laws are the axioms for a mathematical structure known as a Boolean algebra, which is discussed in Section 6.4.

The equivalences of Theorem 2.1.1 are general laws of thought that occur in all areas of human endeavor. They can also be used in a formal way to rewrite complicated statement forms more simply.

Example 2.1.14 **Simplifying Statement Forms**

Use Theorem 2.1.1 to verify the logical equivalence

$$\sim(\sim p \wedge q) \wedge (p \vee q) \equiv p.$$

Solution Use the laws of Theorem 2.1.1 to replace sections of the statement form on the left by logically equivalent expressions. Each time you do this, you obtain a logically equivalent statement form. Continue making replacements until you obtain the statement form on the right.

$$\begin{aligned}
\sim(\sim p \wedge q) \wedge (p \vee q) &\equiv (\sim(\sim p) \vee \sim q) \wedge (p \vee q) && \text{by De Morgan's laws}\\
&\equiv (p \vee \sim q) \wedge (p \vee q) && \text{by the double negative law}\\
&\equiv (p \vee (\sim q \wedge q) && \text{by the distributive law}\\
&\equiv p \vee (q \wedge \sim q) && \text{by the commutative law for } \wedge\\
&\equiv p \vee \mathbf{c} && \text{by the negation law}\\
&\equiv p && \text{by the identity law}
\end{aligned}$$

■

Skill in simplifying statement forms is useful in constructing logically efficient computer programs and in designing digital logic circuits.

Although the properties in Theorem 2.1.1 can be used to prove the logical equivalence of two statement forms, they cannot be used to prove that statement forms are not logically equivalent. On the other hand, truth tables can always be used to determine both equivalence and nonequivalence, and truth tables are easy to program on a computer. When truth tables are used, however, checking for equivalence always requires 2^n steps, where n is the number of variables. Sometimes you can quickly see that two statement forms are equivalent by Theorem 2.1.1, whereas it would take quite a bit of calculating to show their equivalence using truth tables. For instance, it follows immediately from the associative law for $\wedge$ that $p \wedge (\sim q \wedge \sim r) \equiv (p \wedge \sim q) \wedge \sim r$, whereas a truth table verification requires constructing a table with eight rows.

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. An *and* statement is true when, and only when, both components are _____.
2. An *or* statement is false when, and only when, both components are _____.
3. Two statement forms are logically equivalent when, and only when, they always have _____.
4. De Morgan's laws say (1) that the negation of an *and* statement is logically equivalent to the _____ statement in which each component is _____, and (2) that the negation of an *or* statement is logically equivalent to the _____ statement in which each component is _____.
5. A tautology is a statement that is always _____.
6. A contradiction is a statement that is always _____.

EXERCISE SET 2.1*

In each of 1–4 represent the common form of each argument using letters to stand for component sentences, and fill in the blanks so that the argument in part (b) has the same logical form as the argument in part (a).

1. a. If all integers are rational, then the number 1 is rational.
All integers are rational.
Therefore, the number 1 is rational.

b. If all algebraic expressions can be written in prefix notation, then _____.
_____.
Therefore, $(a + 2b)(a^2 - b)$ can be written in prefix notation.

2. a. If all computer programs contain errors, then this program contains an error.
This program does not contain an error.
Therefore, it is not the case that all computer programs contain errors.

b. If _____, then _____.
2 is not odd.
Therefore, it is not the case that all prime numbers are odd.

3. a. This number is even or this number is odd.
This number is not even.
Therefore, this number is odd.

b. _____ or logic is confusing.
My mind is not shot.
Therefore, _____.

4. a. If the program syntax is faulty, then the computer will generate an error message.
If the computer generates an error message, then the program will not run.
Therefore, if the program syntax is faulty, then the program will not run.

b. If this simple graph _____, then it is complete.
If this graph _____, then any two of its vertices can be joined by a path.
Therefore, if this simple graph has 4 vertices and 6 edges, then _____.

5. Indicate which of the following sentences are statements.

a. 1,024 is the smallest four-digit number that is a perfect square.

b. She is a mathematics major.

c. $128 = 2^6$

d. $x = 2^6$

Write the statements in 6–9 in symbolic form using the symbols $\sim$, $\vee$, and $\wedge$ and the indicated letters to represent component statements.

6. Let s = "stocks are increasing" and i = "interest rates are steady."

a. Stocks are increasing but interest rates are steady.

b. Neither are stocks increasing nor are interest rates steady.

7. Juan is a math major but not a computer science major. (m = "Juan is a math major," c = "Juan is a computer science major")

8. Let h = "John is healthy," w = "John is wealthy," and s = "John is wise."

a. John is healthy and wealthy but not wise.

b. John is not wealthy but he is healthy and wise.

c. John is neither healthy, wealthy, nor wise.

d. John is neither wealthy nor wise, but he is healthy.

e. John is wealthy, but he is not both healthy and wise.

9. Let p = "$x > 5$," q = "$x = 5$," and r = "$10 > x$."

a. $x \geq 5$

b. $10 > x > 5$

c. $10 > x \geq 5$

10. Let p be the statement "DATAENDFLAG is off," q the statement "ERROR equals 0," and r the statement "SUM is less than 1,000." Express the following sentences in symbolic notation.

a. DATAENDFLAG is off, ERROR equals 0, and SUM is less than 1,000.

b. DATAENDFLAG is off but ERROR is not equal to 0.

c. DATAENDFLAG is off; however, ERROR is not 0 or SUM is greater than or equal to 1,000.

d. DATAENDFLAG is on and ERROR equals 0 but SUM is greater than or equal to 1,000.

e. Either DATAENDFLAG is on or it is the case that both ERROR equals 0 and SUM is less than 1,000.

11. In the following sentence, is the word *or* used in its inclusive or exclusive sense? A team wins the playoffs if it wins two games in a row or a total of three games.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

Write truth tables for the statement forms in 12–15.

12. $\sim p \wedge q$

13. $\sim(p \wedge q) \vee (p \vee q)$

14. $p \wedge (q \wedge r)$

15. $p \wedge (\sim q \vee r)$

Determine whether the statement forms in 16–24 are logically equivalent. In each case, construct a truth table and include a sentence justifying your answer. Your sentence should show that you understand the meaning of logical equivalence.

16. $p \vee (p \wedge q)$ and p

17. $\sim(p \wedge q)$ and $\sim p \wedge \sim q$

18. $p \vee \mathbf{t}$ and $\mathbf{t}$

19. $p \wedge \mathbf{t}$ and p

20. $p \wedge \mathbf{c}$ and $p \vee \mathbf{c}$

21. $(p \wedge q) \wedge r$ and $p \wedge (q \wedge r)$

22. $p \wedge (q \vee r)$ and $(p \wedge q) \vee (p \wedge r)$

23. $(p \wedge q) \vee r$ and $p \wedge (q \vee r)$

24. $(p \vee q) \vee (p \wedge r)$ and $(p \vee q) \wedge r$

Use De Morgan's laws to write negations for the statements in 25–30.

25. Hal is a math major and Hal's sister is a computer science major.

26. Sam is an orange belt and Kate is a red belt.

27. The connector is loose or the machine is unplugged.

28. The train is late or my watch is fast.

29. This computer program has a logical error in the first ten lines or it is being run with an incomplete data set.

30. The dollar is at an all-time high and the stock market is at a record low.

31. Let s be a string of length 2 with characters from {0, 1, 2}, and define statements a, b, c, and d as follows:

a = "the first character of s is 0"

b = "the first character of s is 1"

c = "the second character of s is 1"

d = "the second character of s is 2".

Describe the set of all strings for which each of the following is true.

a. $(a \vee b) \wedge (c \vee d)$

b. $(\sim(a \vee b)) \wedge (c \vee d)$

c. $((\sim a) \vee b) \wedge (c \vee (\sim d))$

Assume x is a particular real number and use De Morgan's laws to write negations for the statements in 32–37.

32. $-2 < x < 7$

33. $-10 < x < 2$

34. $x < 2$ or $x > 5$

35. $x \leq -1$ or $x > 1$

36. $1 > x \geq -3$

37. $0 > x \geq -7$

In 38 and 39, imagine that *num_orders* and *num_instock* are particular values, such as might occur during execution of a computer program. Write negations for the following statements.

38. (*num_orders* > 100 and *num_instock* ≤ 500) or *num_instock* < 200

39. (*num_orders* < 50 and *num_instock* > 300) or ($50 \leq$ *num_orders* < 75 and *num_instock* > 500)

Use truth tables to establish which of the statement forms in 40–43 are tautologies and which are contradictions.

40. $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$

41. $(p \wedge \sim q) \wedge (\sim p \vee q)$

42. $((\sim p \wedge q) \wedge (q \wedge r)) \wedge \sim q$

43. $(\sim p \vee q) \vee (p \wedge \sim q)$

44. Recall that $a < x < b$ means that $a < x$ and $x < b$. Also $a \leq b$ means that $a < b$ or $a = b$. Find all real numbers that satisfy the following inequalities.

a. $2 < x \leq 0$

b. $1 \leq x < -1$

45. Determine whether the statements in (a) and (b) are logically equivalent.

a. Bob is both a math and computer science major and Ann is a math major, but Ann is not both a math and computer science major.

b. It is not the case that both Bob and Ann are both math and computer science majors, but it is the case that Ann is a math major and Bob is both a math and computer science major.

*46. Let the symbol $\oplus$ denote *exclusive or*; so $p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$. Hence the truth table for $p \oplus q$ is as follows:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

a. Find simpler statement forms that are logically equivalent to $p \oplus p$ and $(p \oplus p) \oplus p$.
b. Is $(p \oplus q) \oplus r \equiv p \oplus (q \oplus r)$? Justify your answer.
c. Is $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$? Justify your answer.

*47. In logic and in standard English, a double negative is equivalent to a positive. There is one fairly common English usage in which a "double positive" is equivalent to a negative. What is it? Can you think of others?

In 48 and 49 below, a logical equivalence is derived from Theorem 2.1.1. Supply a reason for each step.

48. $(p \wedge \sim q) \vee (p \wedge q) \equiv p \wedge (\sim q \vee q)$ by (a)
$\equiv p \wedge (q \vee \sim q)$ by (b)
$\equiv p \wedge \mathbf{t}$ by (c)
$\equiv p$ by (d)
Therefore, $(p \wedge \sim q) \vee (p \wedge q) \equiv p$.

49. $(p \vee \sim q) \wedge (\sim p \vee \sim q)$
$\equiv (\sim q \vee p) \wedge (\sim q \vee \sim p)$ by (a)
$\equiv \sim q \vee (p \wedge \sim p)$ by (b)
$\equiv \sim q \vee \mathbf{c}$ by (c)
$\equiv \sim q$ by (d)
Therefore, $(p \vee \sim q) \wedge (\sim p \vee \sim q) \equiv \sim q$.

Use Theorem 2.1.1 to verify the logical equivalences in 50–54. Supply a reason for each step.

50. $(p \wedge \sim q) \vee p \equiv p$

51. $p \wedge (\sim q \vee p) \equiv p$

52. $\sim(p \vee \sim q) \vee (\sim p \wedge \sim q) \equiv \sim p$

53. $\sim((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \vee (p \wedge q) \equiv p$

54. $(p \wedge (\sim(\sim p \vee q))) \vee (p \wedge q) \equiv p$

ANSWERS FOR TEST YOURSELF

1. true 2. false 3. the same truth values 4. *or*; negated; *and*; negated 5. true 6. false

2.2 Conditional Statements

. . . hypothetical reasoning implies the subordination of the real to the realm of the possible . . . —Jean Piaget, 1972

When you make a logical inference or deduction, you reason *from* a hypothesis *to* a conclusion. Your aim is to be able to say, "*If* such and such is known, *then* something or other must be the case."

Let p and q be statements. A sentence of the form "If p then q" is denoted symbolically by "$p \rightarrow q$"; p is called the *hypothesis* and q is called the *conclusion*. For instance, consider the following statement:

If $\underbrace{\text{4,686 is divisible by 6}}_{\text{hypothesis}}$, then $\underbrace{\text{4,686 is divisible by 3}}_{\text{conclusion}}$

Such a sentence is called *conditional* because the truth of statement q is conditioned on the truth of statement p.

The notation $p \rightarrow q$ indicates that $\rightarrow$ is a connective, like $\wedge$ or $\vee$, which can be used to join statements to create new statements. To define $p \rightarrow q$ as a statement, therefore, we must specify the truth values for $p \rightarrow q$ as we specified truth values for $p \wedge q$ and for $p \vee q$. As is the case with the other connectives, the formal definition of truth values for $\rightarrow$ (if-then) is based on its everyday, intuitive meaning. Consider an example.

Suppose you go to interview for a job at a store and the owner of the store makes you the following promise:

If you show up for work Monday morning, then you will get the job.

Under what circumstances are you justified in saying the owner spoke falsely? That is, under what circumstances is the above sentence false? The answer is: You *do* show up for work Monday morning and you do *not* get the job.

After all, the owner's promise only says you will get the job *if* a certain condition (showing up for work Monday morning) is met; it says nothing about what will happen if the condition is *not* met. So if the condition is not met, you cannot in fairness say the promise is false regardless of whether or not you get the job.

The above example was intended to convince you that *the only combination of circumstances in which you would call a conditional sentence false occurs when the hypothesis is true and the conclusion is false*. In all other cases, you would not call the sentence false. This implies that the only row of the truth table for $p \rightarrow q$ that should be filled in with an F is the row where p is T and q is F. No other row should contain an F. But each row of a truth table must be filled in with either a T or an F. Thus all other rows of the truth table for $p \rightarrow q$ must be filled in with T's.

Truth Table for $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Definition

If p and q are statement variables, the **conditional** of q by p is "If p then q" or "p implies q" and is denoted $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We call p the **hypothesis** (or **antecedent**) of the conditional and q the **conclusion** (or **consequent**).

A conditional statement that is true by virtue of the fact that its hypothesis is false is often called **vacuously true** or **true by default**. Thus the statement "If you show up for work Monday morning, then you will get the job" is vacuously true if you do not show up for work Monday morning. In general, when the "if" part of an if-then statement is false, the statement as a whole is said to be true, regardless of whether the conclusion is true or false.

Example 2.2.1 **A Conditional Statement with a False Hypothesis**

Consider the statement

If $0 = 1$ then $1 = 2$.

As strange as it may seem, since the hypothesis of this statement is false, the statement as a whole is true. ■

Note For example, if you hypothesize that $0 = 1$, then, by adding 1 to both sides of the equation, you can deduce that $1 = 2$.

The philosopher Willard Van Orman Quine advises against using the phrase "p implies q" to mean "$p \rightarrow q$" because the word *implies* suggests that q can be logically deduced from p and this is often not the case. Nonetheless, the phrase is used by many people, probably because it is a convenient replacement for the $\rightarrow$ symbol. And, of course, in many cases a conclusion can be deduced from a hypothesis, even when the hypothesis is false.

In expressions that include $\rightarrow$ as well as other logical operators such as $\wedge$, $\vee$, and $\sim$, the **order of operations** is that $\rightarrow$ is performed last. Thus, according to the specification of order of operations in Section 2.1, $\sim$ is performed first, then $\wedge$ and $\vee$, and finally $\rightarrow$.

Example 2.2.2 **Truth Table for $p \vee \sim q \rightarrow \sim p$**

Construct a truth table for the statement form $p \vee \sim q \rightarrow \sim p$.

Solution By the order of operations given above, the following two expressions are equivalent: $p \vee \sim q \rightarrow \sim p$ and $(p \vee (\sim q)) \rightarrow (\sim p)$, and this order governs the construction of the truth table. First fill in the four possible combinations of truth values for p and q, and then enter the truth values for $\sim p$ and $\sim q$ using the definition of negation. Next fill in the $p \vee \sim q$ column using the definition of $\vee$. Finally, fill in the $p \vee \sim q \rightarrow \sim p$ column using the definition of $\rightarrow$.

Note The only rows in which the hypothesis $p \vee \sim q$ is true and the conclusion $\sim p$ is false are the first and second rows. So you put F's in those two rows and T's in the other two rows.

		conclusion		hypothesis	
p	q	$\sim p$	$\sim q$	$p \vee \sim q$	$p \vee \sim q \rightarrow \sim p$
T	T	F	F	T	F
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	T	T

■

Logical Equivalences Involving $\rightarrow$

Imagine that you are trying to solve a problem involving three statements: p, q, and r. Suppose you know that the truth of r follows from the truth of p *and also* that the truth of r follows from the truth of q. Then no matter whether p or q is the case, the truth of r must follow. The division-into-cases method of analysis is based on this idea.

Example 2.2.3 **Division into Cases: Showing That $p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$**

Use truth tables to show the logical equivalence of the statement forms $p \vee q \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$. Annotate the table with a sentence of explanation.

Solution First fill in the eight possible combinations of truth values for p, q, and r. Then fill in the columns for $p \vee q$, $p \rightarrow r$, and $q \rightarrow r$ using the definitions of *or* and *if-then*. For instance, the $p \rightarrow r$ column has F's in the second and fourth rows because these are the rows in which p is true and r is false. Next fill in the $p \vee q \rightarrow r$ column using the definition of *if-then*. The rows in which the hypothesis $p \vee q$ is true and the conclusion r is false are the second, fourth, and sixth. So F's go in these rows and T's in all the others. The complete table shows that $p \vee q \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$ have the same truth values for each combination of truth values of p, q, and r. Hence the two statement forms are logically equivalent.

p	q	r	$p \vee q$	$p \rightarrow r$	$q \rightarrow r$	$p \vee q \rightarrow r$	$(p \rightarrow r) \wedge (q \rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	T	T	T	T	T
F	T	F	T	T	F	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

$p \vee q \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$ always have the same truth values, so they are logically equivalent ■

Representation of If-Then as Or

In exercise 13(a) at the end of this section you are asked to use truth tables to show that

$$p \rightarrow q \equiv \sim p \vee q.$$

The logical equivalence of "if p then q" and "not p or q" is occasionally used in everyday speech. Here is one instance.

Example 2.2.4 **Application of the Equivalence between $\sim p \vee q$ and $p \rightarrow q$**

Rewrite the following statement in if-then form.

Either you get to work on time or you are fired.

Solution Let $\sim p$ be

You get to work on time.

and q be

You are fired.

Then the given statement is $\sim p \vee q$. Also p is

You do not get to work on time.

So the equivalent if-then version, $p \rightarrow q$, is

If you do not get to work on time, then you are fired. ■

The Negation of a Conditional Statement

By definition, $p \rightarrow q$ is false if, and only if, its hypothesis, p, is true and its conclusion, q, is false. It follows that

> The negation of "if p then q" is logically equivalent to "p and not q."

This can be restated symbolically as follows:

$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

To obtain this result you can also start from the logical equivalence $p \rightarrow q \equiv \sim p \vee q$. Take the negation of both sides to obtain

$$\begin{aligned} \sim(p \rightarrow q) &\equiv \sim(\sim p \vee q) \\ &\equiv \sim(\sim p) \wedge (\sim q) && \text{by De Morgan's laws} \\ &\equiv p \wedge \sim q && \text{by the double negative law.} \end{aligned}$$

Yet another way to derive this result is to construct truth tables for $\sim(p \rightarrow q)$ and for $p \wedge \sim q$ and to check that they have the same truth values. (See exercise 13(b) at the end of this section.)

Example 2.2.5 **Negations of *If-Then* Statements**

Write negations for each of the following statements:

a. If my car is in the repair shop, then I cannot get to class.

b. If Sara lives in Athens, then she lives in Greece.

Solution

a. My car is in the repair shop and I can get to class.

b. Sara lives in Athens and she does not live in Greece. (Sara might live in Athens, Georgia; Athens, Ohio; or Athens, Wisconsin.) ■

Caution! Remember that **the negation of an if-then statement does not start with the word *if*.**

It is tempting to write the negation of an if-then statement as another if-then statement. Please resist that temptation!

The Contrapositive of a Conditional Statement

One of the most fundamental laws of logic is the equivalence between a conditional statement and its contrapositive.

Definition

The **contrapositive** of a conditional statement of the form "If p then q" is

If $\sim q$ then $\sim p$.

Symbolically,

The contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.

The fact is that

A conditional statement is logically equivalent to its contrapositive.

You are asked to establish this equivalence in exercise 26 at the end of this section.

Example 2.2.6 **Writing the Contrapositive**

Write each of the following statements in its equivalent contrapositive form:

a. If Howard can swim across the lake, then Howard can swim to the island.

b. If today is Easter, then tomorrow is Monday.

Solution

a. If Howard cannot swim to the island, then Howard cannot swim across the lake.

b. If tomorrow is not Monday, then today is not Easter. ■

When you are trying to solve certain problems, you may find that the contrapositive form of a conditional statement is easier to work with than the original statement. Replacing a statement by its contrapositive may give the extra push that helps you over the top in your search for a solution. This logical equivalence is also the basis for one of the most important laws of deduction, modus tollens (to be explained in Section 2.3), and for the contrapositive method of proof (to be explained in Section 4.7).

The Converse and Inverse of a Conditional Statement

The fact that a conditional statement and its contrapositive are logically equivalent is very important and has wide application. Two other variants of a conditional statement are *not* logically equivalent to the statement.

Definition

Suppose a conditional statement of the form "If p then q" is given.

1. The **converse** is "If q then p."
2. The **inverse** is "If $\sim p$ then $\sim q$."

Symbolically,

$$\text{The converse of } p \to q \text{ is } q \to p,$$

and

$$\text{The inverse of } p \to q \text{ is } \sim p \to \sim q.$$

Example 2.2.7 **Writing the Converse and the Inverse**

Write the converse and inverse of each of the following statements:

a. If Howard can swim across the lake, then Howard can swim to the island.

b. If today is Easter, then tomorrow is Monday.

Solution

a. *Converse:* If Howard can swim to the island, then Howard can swim across the lake.
Inverse: If Howard cannot swim across the lake, then Howard cannot swim to the island.

b. *Converse:* If tomorrow is Monday, then today is Easter.
Inverse: If today is not Easter, then tomorrow is not Monday. ■

Caution! Many people believe that if a conditional statement is true, then its converse and inverse must also be true. This is not correct! The converse might be true, but it does not have to be true.

Note that while the statement "If today is Easter, then tomorrow is Monday" is always true, both its converse and inverse are false on every Sunday except Easter.

1. A conditional statement and its converse are *not* logically equivalent.
2. A conditional statement and its inverse are *not* logically equivalent.
3. The converse and the inverse of a conditional statement are logically equivalent to each other.

In exercises 24, 25, and 27 at the end of this section, you are asked to use truth tables to verify the statements in the box above. Note that the truth of statement 3 also follows from the observation that the inverse of a conditional statement is the contrapositive of its converse.

Only If and the Biconditional

To say "p only if q" means that p can take place *only* if q takes place also. That is, if q does not take place, then p cannot take place. Another way to say this is that if p occurs, then q must also occur (by the logical equivalence between a statement and its contrapositive).

Definition

If p and q are statements,

p **only if** q means "if not q then not p,"

or, equivalently,

"if p then q."

Example 2.2.8 **Converting *Only If* to *If-Then***

Rewrite the following statement in if-then form in two ways, one of which is the contrapositive of the other.

> John will break the world's record for the mile run only if he runs the mile in under four minutes.

Solution *Version 1:* If John does not run the mile in under four minutes, then he will not break the world's record.

Version 2: If John breaks the world's record, then he will have run the mile in under four minutes. ■

Caution! "p only if q" does *not* mean "p if q."

Note that it is possible for "p only if q" to be true at the same time that "p if q" is false. For instance, to say that John will break the world's record only if he runs the mile in under four minutes does not mean that John will break the world's record if he runs the mile in under four minutes. His time could be under four minutes but still not be fast enough to break the record.

Definition

Given statement variables p and q, the **biconditional of p and q** is "p if, and only if, q" and is denoted $p \leftrightarrow q$. It is true if both p and q have the same truth values and is false if p and q have opposite truth values. The words *if and only if* are sometimes abbreviated **iff**.

The biconditional has the following truth table:

Truth Table for $p \leftrightarrow q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

In order of operations $\leftrightarrow$ is coequal with $\rightarrow$. As with $\wedge$ and $\vee$, the only way to indicate precedence between them is to use parentheses. The full hierarchy of operations for the five logical operators is shown below.

Order of Operations for Logical Operators

1. $\sim$ Evaluate negations first.
2. $\wedge, \vee$ Evaluate $\wedge$ and $\vee$ second. When both are present, parentheses may be needed.
3. $\rightarrow, \leftrightarrow$ Evaluate $\rightarrow$ and $\leftrightarrow$ third. When both are present, parentheses may be needed.

According to the separate definitions of *if* and *only if*, saying "p if, and only if, q" should mean the same as saying both "p if q" and "p only if q." The following annotated truth table shows that this is the case:

Truth Table Showing That $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

$p \leftrightarrow q$ and $(p \rightarrow q) \wedge (q \rightarrow p)$ always have the same truth values, so they are logically equivalent

Example 2.2.9 ***If* and *Only If***

Rewrite the following statement as a conjunction of two if-then statements:

> This computer program is correct if, and only if, it produces correct answers for all possible sets of input data.

Solution If this program is correct, then it produces the correct answers for all possible sets of input data; and if this program produces the correct answers for all possible sets of input data, then it is correct. ■

Necessary and Sufficient Conditions

The phrases *necessary condition* and *sufficient condition*, as used in formal English, correspond exactly to their definitions in logic.

Definition

If r and s are statements:

r is a **sufficient condition** for s means "if r then s."

r is a **necessary condition** for s means "if not r then not s."

In other words, to say "r is a sufficient condition for s" means that the occurrence of r is *sufficient* to guarantee the occurrence of s. On the other hand, to say "r is a necessary condition for s" means that if r does not occur, then s cannot occur either:

> The occurrence of r is *necessary* to obtain the occurrence of s. Note that because of the equivalence between a statement and its contrapositive,
>
> r is a necessary condition for s also means "if s then r."
>
> Consequently,
>
> r is a necessary and sufficient condition for s means "r if, and only if, s."

Example 2.2.10 **Interpreting Necessary and Sufficient Conditions**

Consider the statement "If John is eligible to vote, then he is at least 18 years old." The truth of the condition "John is eligible to vote" is *sufficient* to ensure the truth of the condition "John is at least 18 years old." In addition, the condition "John is at least 18 years old" is *necessary* for the condition "John is eligible to vote" to be true. If John were younger than 18, then he would not be eligible to vote. ■

Example 2.2.11 **Converting a Sufficient Condition to If-Then Form**

Rewrite the following statement in the form "If A then B":

> Pia's birth on U.S. soil is a sufficient condition for her to be a U.S. citizen.

Solution If Pia was born on U.S. soil, then she is a U.S. citizen. ■

Example 2.2.12 **Converting a Necessary Condition to If-Then Form**

Use the contrapositive to rewrite the following statement in two ways:

> George's attaining age 35 is a necessary condition for his being president of the United States.

Solution *Version 1:* If George has not attained the age of 35, then he cannot be president of the United States.
Version 2: If George can be president of the United States, then he has attained the age of 35. ■

Remarks

1. *In logic, a hypothesis and conclusion are not required to have related subject matters.*
   In ordinary speech we never say things like "If computers are machines, then Babe Ruth was a baseball player" or "If $2 + 2 = 5$, then Mickey Mouse is president of the United States." We formulate a sentence like "If p then q" only if there is some connection of content between p and q.
   In logic, however, the two parts of a conditional statement need not have related meanings. The reason? If there were such a requirement, who would enforce it? What one person perceives as two unrelated clauses may seem related to someone else. There would have to be a central arbiter to check each conditional sentence before anyone could use it, to be sure its clauses were in proper relation. This is impractical, to say the least!
   Thus a statement like "if computers are machines, then Babe Ruth was a baseball player" is allowed, and it is even called true because both its hypothesis and its conclusion are true. Similarly, the statement "If $2 + 2 = 5$, then Mickey Mouse is president of the United States" is allowed and is called true because its hypothesis is false, even though doing so may seem ridiculous.
   In mathematics it often happens that a carefully formulated definition that successfully covers the situations for which it was primarily intended is later seen to be satisfied by some extreme cases that the formulator did not have in mind. But those are the breaks, and it is important to get into the habit of exploring definitions fully to seek out and understand *all* their instances, even the unusual ones.

2. *In informal language, simple conditionals are often used to mean biconditionals.*
   The formal statement "p if, and only if, q" is seldom used in ordinary language. Frequently, when people intend the biconditional they leave out either the *and only if* or the *if and*. That is, they say either "p if q" or "p only if q" when they really mean "p if, and only if, q." For example, consider the statement "You will get dessert if, and only if, you eat your dinner." Logically, this is equivalent to the conjunction of the following two statements.

   Statement 1: If you eat your dinner, then you will get dessert.
   Statement 2: You will get dessert only if you eat your dinner.
   or
   If you do not eat your dinner, then you will not get dessert.

   Now how many parents in the history of the world have said to their children "You will get dessert if, and only if, you eat your dinner"? Not many! Most say either "If you eat your dinner, you will get dessert" (these take the positive approach—they emphasize the reward) or "You will get dessert only if you eat your dinner" (these take the

negative approach—they emphasize the punishment). Yet the parents who promise the reward intend to suggest the punishment as well, and those who threaten the punishment will certainly give the reward if it is earned. Both sets of parents expect that their conditional statements will be interpreted as biconditionals.

Since we often (correctly) interpret conditional statements as biconditionals, it is not surprising that we may come to believe (mistakenly) that conditional statements are always logically equivalent to their inverses and converses. In formal settings, however, statements must have unambiguous interpretations. If-then statements can't sometimes mean "if-then" and other times mean "if and only if." When using language in mathematics, science, or other situations where precision is important, it is essential to interpret if-then statements according to the formal definition and not to confuse them with their converses and inverses.

TEST YOURSELF

1. An *if-then* statement is false if, and only if, the hypothesis is _____ and the conclusion is _____.
2. The negation of "if p then q" is _____.
3. The converse of "if p then q" is _____.
4. The contrapositive of "if p then q" is _____.
5. The inverse of "if p then q" is _____.
6. A conditional statement and its contrapositive are _____.
7. A conditional statement and its converse are not _____.
8. "R is a sufficient condition for S" means "if _____ then _____."
9. "R is a necessary condition for S" means "if _____ then _____."
10. "R only if S" means "if _____ then _____."

EXERCISE SET 2.2

Rewrite the statements in 1–4 in if-then form.

1. This loop will repeat exactly N times if it does not contain a **stop** or a **go to**.
2. I am on time for work if I catch the 8:05 bus.
3. Freeze or I'll shoot.
4. Fix my ceiling or I won't pay my rent.

Construct truth tables for the statement forms in 5–11.

5. $\sim p \vee q \rightarrow \sim q$
6. $(p \vee q) \vee (\sim p \wedge q) \rightarrow q$
7. $p \wedge \sim q \rightarrow r$
8. $\sim p \vee q \rightarrow r$
9. $p \wedge \sim r \leftrightarrow q \vee r$
10. $(p \rightarrow r) \leftrightarrow (q \rightarrow r)$
11. $(p \rightarrow (q \rightarrow r)) \leftrightarrow ((p \wedge q) \rightarrow r)$
12. Use the logical equivalence established in Example 2.2.3, $p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$, to rewrite the following statement. (Assume that x represents a fixed real number.)

    If $x > 2$ or $x < -2$, then $x^2 > 4$.

13. Use truth tables to verify the following logical equivalences. Include a few words of explanation with your answers.
    a. $p \rightarrow q \equiv \sim p \vee q$
    b. $\sim(p \rightarrow q) \equiv p \wedge \sim q$.

H 14. a. Show that the following statement forms are all logically equivalent:

$$p \rightarrow q \vee r, \quad p \wedge \sim q \rightarrow r, \quad \text{and} \quad p \wedge \sim r \rightarrow q$$

    b. Use the logical equivalences established in part (a) to rewrite the following sentence in two different ways. (Assume that n represents a fixed integer.)

    If n is prime, then n is odd or n is 2.

15. Determine whether the following statement forms are logically equivalent:

$$p \to (q \to r) \quad \text{and} \quad (p \to q) \to r$$

In 16 and 17, write each of the two statements in symbolic form and determine whether they are logically equivalent. Include a truth table and a few words of explanation to show that you understand what it means for statements to be logically equivalent.

16. If you paid full price, you didn't buy it at Crown Books. You didn't buy it at Crown Books or you paid full price.

17. If 2 is a factor of n and 3 is a factor of n, then 6 is a factor of n. 2 is not a factor of n or 3 is not a factor of n or 6 is a factor of n.

18. Write each of the following three statements in symbolic form and determine which pairs are logically equivalent. Include truth tables and a few words of explanation.

If it walks like a duck and it talks like a duck, then it is a duck.

Either it does not walk like a duck or it does not talk like a duck, or it is a duck.

If it does not walk like a duck and it does not talk like a duck, then it is not a duck.

19. True or false? The negation of "If Sue is Luiz's mother, then Ali is his cousin" is "If Sue is Luiz's mother, then Ali is not his cousin."

20. Write negations for each of the following statements. (Assume that all variables represent fixed quantities or entities, as appropriate.)

a. If P is a square, then P is a rectangle.
b. If today is New Year's Eve, then tomorrow is January.
c. If the decimal expansion of r is terminating, then r is rational.
d. If n is prime, then n is odd or n is 2.
e. If x is nonnegative, then x is positive or x is 0.
f. If Tom is Ann's father, then Jim is her uncle and Sue is her aunt.
g. If n is divisible by 6, then n is divisible by 2 and n is divisible by 3.

21. Suppose that p and q are statements so that $p \to q$ is false. Find the truth values of each of the following:

a. $\sim p \to q$ **b.** $p \vee q$ **c.** $q \to p$

***H* 22.** Write contrapositives for the statements of exercise 20.

***H* 23.** Write the converse and inverse for each statement of exercise 20.

Use truth tables to establish the truth of each statement in 24–27.

24. A conditional statement is not logically equivalent to its converse.

25. A conditional statement is not logically equivalent to its inverse.

26. A conditional statement and its contrapositive are logically equivalent to each other.

27. The converse and inverse of a conditional statement are logically equivalent to each other.

***H* 28.** "Do you mean that you think you can find out the answer to it?" said the March Hare.

"Exactly so," said Alice.

"Then you should say what you mean," the March Hare went on.

"I do," Alice hastily replied; "at least—at least I mean what I say—that's the same thing, you know."

"Not the same thing a bit!" said the Hatter. "Why, you might just as well say that 'I see what I eat' is the same thing as 'I eat what I see'!"

—from "A Mad Tea-Party" in *Alice in Wonderland*, by Lewis Carroll

The Hatter is right. "I say what I mean" is not the same thing as "I mean what I say." Rewrite each of these two sentences in if-then form and explain the logical relation between them. (This exercise is referred to in the introduction to Chapter 4.)

If statement forms *P* and *Q* are logically equivalent, then $P \leftrightarrow Q$ is a tautology. Conversely, if $P \leftrightarrow Q$ is a tautology, then *P* and *Q* are logically equivalent. Use $\leftrightarrow$ to convert each of the logical equivalences in 29–31 to a tautology. Then use a truth table to verify each tautology.

29. $p \to (q \vee r) \equiv (p \wedge \sim q) \to r$

30. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

31. $p \to (q \to r) \equiv (p \wedge q) \to r$

Rewrite each of the statements in 32 and 33 as a conjunction of two if-then statements.

32. This quadratic equation has two distinct real roots if, and only if, its discriminant is greater than zero.

33. This integer is even if, and only if, it equals twice some integer.

Rewrite the statements in 34 and 35 in if-then form in two ways, one of which is the contrapositive of the other. Use the formal definition of "only if."

34. The Cubs will win the pennant only if they win tomorrow's game.

35. Sam will be allowed on Signe's racing boat only if he is an expert sailor.

36. Taking the long view on your education, you go to the Prestige Corporation and ask what you should do in college to be hired when you graduate. The personnel director replies that you will be hired *only if* you major in mathematics or computer science, get a B average or better, and take accounting. You do, in fact, become a math major, get a B+ average, and take accounting. You return to Prestige Corporation, make a formal application, and are turned down. Did the personnel director lie to you?

Some programming languages use statements of the form "*r* unless *s*" to mean that as long as *s* does not happen, then *r* will happen. More formally:

> **Definition:** If r and s are statements,
>
> ***r* unless *s*** means if $\sim s$ then r.

In 37–39, rewrite the statements in if-then form.

37. Payment will be made on fifth unless a new hearing is granted.

38. Ann will go unless it rains.

39. This door will not open unless a security code is entered.

Rewrite the statements in 40 and 41 in if-then form.

40. Catching the 8:05 bus is a sufficient condition for my being on time for work.

41. Having two 45° angles is a sufficient condition for this triangle to be a right triangle.

Use the contrapositive to rewrite the statements in 42 and 43 in if-then form in two ways.

42. Being divisible by 3 is a necessary condition for this number to be divisible by 9.

43. Doing homework regularly is a necessary condition for Jim to pass the course.

Note that "a sufficient condition for *s* is *r*" means *r* is a sufficient condition for *s* and that "a necessary condition for *s* is *r*" means *r* is a necessary condition for *s*. Rewrite the statements in 44 and 45 in if-then form.

44. A sufficient condition for Jon's team to win the championship is that it win the rest of its games.

45. A necessary condition for this computer program to be correct is that it not produce error messages during translation.

46. "If compound X is boiling, then its temperature must be at least 150°C." Assuming that this statement is true, which of the following must also be true?

- **a.** If the temperature of compound X is at least 150°C, then compound X is boiling.
- **b.** If the temperature of compound X is less than 150°C, then compound X is not boiling.
- **c.** Compound X will boil only if its temperature is at least 150°C.
- **d.** If compound X is not boiling, then its temperature is less than 150°C.
- **e.** A necessary condition for compound X to boil is that its temperature be at least 150°C.
- **f.** A sufficient condition for compound X to boil is that its temperature be at least 150°C.

In 47–50 (a) use the logical equivalences $p \to q \equiv \sim p \vee q$ and $p \leftrightarrow q \equiv (\sim p \vee q) \wedge (\sim q \vee p)$ to rewrite the given statement forms without using the symbol $\to$ or $\leftrightarrow$, and (b) use the logical equivalence $p \vee q \equiv \sim(\sim p \wedge \sim q)$ to rewrite each statement form using only $\wedge$ and $\sim$.

47. $p \wedge \sim q \to r$

48. $p \vee \sim q \to r \vee q$

49. $(p \to r) \leftrightarrow (q \to r)$

50. $(p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$

51. Given any statement form, is it possible to find a logically equivalent form that uses only $\sim$ and $\wedge$? Justify your answer.

ANSWERS FOR TEST YOURSELF

1. true; false **2.** $p \wedge \sim q$ **3.** if q then p **4.** if $\sim q$ then $\sim p$ **5.** if $\sim p$ then $\sim q$ **6.** logically equivalent **7.** logically equivalent **8.** R; S **9.** S; R **10.** R; S

2.3 Valid and Invalid Arguments

"Contrariwise," continued Tweedledee, "if it was so, it might be; and if it were so, it would be; but as it isn't, it ain't. That's logic." —Lewis Carroll, *Through the Looking Glass*

In mathematics and logic an argument is not a dispute. It is simply a sequence of statements ending in a conclusion. In this section we show how to determine whether an argument is valid—that is, whether the conclusion follows *necessarily* from the preceding statements. We will show that this determination depends only on the form of an argument, not on its content.

It was shown in Section 2.1 that the logical form of an argument can be abstracted from its content. For example, the argument

If Socrates is a man, then Socrates is mortal.
Socrates is a man.
$\therefore$ Socrates is mortal.

has the abstract form

If p then q
p
$\therefore q$

When considering the abstract form of an argument, think of p and q as variables for which statements may be substituted. An argument form is called *valid* if, and only if, whenever statements are substituted that make all the premises true, the conclusion is also true.

Definition

An **argument** is a sequence of statements, and an **argument form** is a sequence of statement forms. All statements in an argument and all statement forms in an argument form, except for the final one, are called **premises** (or **assumptions** or **hypotheses**). The final statement or statement form is called the **conclusion**. The symbol $\therefore$, which is read "therefore," is normally placed just before the conclusion.

To say that an *argument form* is **valid** means that no matter what particular statements are substituted for the statement variables in its premises, if the resulting premises are all true, then the conclusion is also true. To say that an *argument* is **valid** means that its form is valid.

The crucial fact about a valid argument is that the truth of its conclusion follows *necessarily* or *inescapably* or *by logical form alone* from the truth of its premises. It is impossible to have a valid argument with all true premises and a false conclusion. When an argument is valid and its premises are true, the truth of the conclusion is said to be *inferred*

or *deduced* from the truth of the premises. If a conclusion "ain't necessarily so," then it isn't a valid deduction.

Testing an Argument Form for Validity

1. Identify the premises and conclusion of the argument form.
2. Construct a truth table showing the truth values of all the premises and the conclusion.
3. A row of the truth table in which all the premises are true is called a **critical row**. If there is a critical row in which the conclusion is false, then it is possible for an argument of the given form to have true premises and a false conclusion, and so the argument form is invalid. If the conclusion in *every* critical row is true, then the argument form is valid.

Example 2.3.1 **Determining Validity or Invalidity**

Determine whether the following argument form is valid or invalid by drawing a truth table, indicating which columns represent the premises and which represent the conclusion, and annotating the table with a sentence of explanation. When you fill in the table, you only need to indicate the truth values for the conclusion in the rows where all the premises are true (the critical rows) because the truth values of the conclusion in the other rows are irrelevant to the validity or invalidity of the argument.

$$p \to q \vee \sim r$$
$$q \to p \wedge r$$
$$\therefore p \to r$$

Caution! If at least one premise of an argument is false, then we have no information about the conclusion: It might be true or it might be false.

Solution The truth table shows that even though there are several situations in which the premises and the conclusion are all true (rows 1, 7, and 8), there is one situation (row 4) where the premises are true and the conclusion is false.

						premises		conclusion
p	q	r	$\sim r$	$q \vee \sim r$	$p \wedge r$	$p \to q \vee \sim r$	$q \to p \wedge r$	$p \to r$
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	
T	F	T	F	F	T	F	T	
T	F	F	T	T	F	T	T	F
F	T	T	F	T	F	T	F	
F	T	F	T	T	F	T	F	
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

This row shows that an argument of this form can have true premises and a false conclusion. Hence this form of argument is invalid.

■

Modus Ponens and Modus Tollens

An argument form consisting of two premises and a conclusion is called a **syllogism**. The first and second premises are called the **major premise** and **minor premise**, respectively. The most famous form of syllogism in logic is called **modus ponens**. It has the following form:

If p then q.
p
$\therefore q$

Here is an argument of this form:

If the sum of the digits of 371,487 is divisible by 3, then 371,487 is divisible by 3.
The sum of the digits of 371,487 is divisible by 3.
$\therefore$ 371,487 is divisible by 3.

The term *modus ponens* is Latin meaning "method of affirming" (the conclusion is an affirmation). Long before you saw your first truth table, you were undoubtedly being convinced by arguments of this form. Nevertheless, it is instructive to prove that modus ponens is a valid form of argument, if for no other reason than to confirm the agreement between the formal definition of validity and the intuitive concept. To do so, we construct a truth table for the premises and conclusion.

		premises		conclusion	
p	q	$p \rightarrow q$	p	q	
T	T	T	T	T	← critical row
T	F	F	T		
F	T	T	F		
F	F	T	F		

The first row is the only one in which both premises are true, and the conclusion in that row is also true. Hence the argument form is valid.

Now consider another valid argument form called **modus tollens**. It has the following form:

If p then q.
$\sim q$
$\therefore \sim p$

Here is an example of modus tollens:

If Zeus is human, then Zeus is mortal.
Zeus is not mortal.
$\therefore$ Zeus is not human.

An intuitive explanation for the validity of modus tollens uses proof by contradiction. It goes like this:

Suppose

(1) If Zeus is human, then Zeus is mortal; and

(2) Zeus is not mortal.

Must Zeus necessarily be nonhuman?

Yes!

Because, if Zeus were human, then by (1) he would be mortal.

But by (2) he is not mortal.

Hence, Zeus cannot be human.

Modus tollens is Latin meaning "method of denying" (the conclusion is a denial). The validity of modus tollens can be shown to follow from modus ponens together with the fact that a conditional statement is logically equivalent to its contrapositive. Or it can be established formally by using a truth table. (See exercise 13.)

Studies by cognitive psychologists have shown that although nearly 100% of college students have a solid, intuitive understanding of modus ponens, less than 60% are able to apply modus tollens correctly.* Yet in mathematical reasoning, modus tollens is used almost as often as modus ponens. Thus it is important to study the form of modus tollens carefully to learn to use it effectively.

Example 2.3.2 **Recognizing Modus Ponens and Modus Tollens**

Use modus ponens or modus tollens to fill in the blanks of the following arguments so that they become valid inferences.

a. If there are more pigeons than there are pigeonholes, then at least two pigeons roost in the same hole.
There are more pigeons than there are pigeonholes.
$\therefore$ _____.

b. If 870,232 is divisible by 6, then it is divisible by 3.
870,232 is not divisible by 3.
$\therefore$ _____.

Solution

a. At least two pigeons roost in the same hole. by modus ponens

b. 870,232 is not divisible by 6. by modus tollens ■

Additional Valid Argument Forms: Rules of Inference

A **rule of inference** is a form of argument that is valid. Thus modus ponens and modus tollens are both rules of inference. The following are additional examples of rules of inference that are frequently used in deductive reasoning.

Example 2.3.3 **Generalization**

The following argument forms are valid:

a. p
$\therefore p \vee q$

b. q
$\therefore p \vee q$

**Cognitive Psychology and Its Implications*, 3d ed. by John R. Anderson (New York: Freeman, 1990), pp. 292–297.

These argument forms are used for making generalizations. For instance, according to the first, if p is true, then, more generally, "p or q" is true for *any* other statement q. As an example, suppose you are given the job of counting the upperclassmen at your school. You ask what class Anton is in and are told he is a junior.

You reason as follows:

Anton is a junior.
$\therefore$ (more generally) Anton is a junior or Anton is a senior.

Knowing that upperclassman means junior or senior, you add Anton to your list. ■

Example 2.3.4 **Specialization**

The following argument forms are valid:

a. $p \wedge q$ $\therefore p$ b. $p \wedge q$ $\therefore q$

These argument forms are used for specializing. When classifying objects according to some property, you often know much more about them than whether they do or do not have that property. When this happens, you discard extraneous information as you concentrate on the particular property of interest.

For instance, suppose you are looking for a person who knows graph algorithms to work with you on a project. You discover that Ana knows both numerical analysis and graph algorithms. You reason as follows:

Ana knows numerical analysis and Ana knows graph algorithms.
$\therefore$ (in particular) Ana knows graph algorithms.

Accordingly, you invite her to work with you on your project. ■

Both generalization and specialization are used frequently in mathematics to tailor facts to fit into hypotheses of known theorems in order to draw further conclusions. Elimination, transitivity, and proof by division into cases are also widely used tools.

Example 2.3.5 **Elimination**

The following argument forms are valid:

a. $p \vee q$ $\sim q$ $\therefore p$ b. $p \vee q$ $\sim p$ $\therefore q$

These argument forms say that when you have only two possibilities and you can rule one out, the other must be the case. For instance, suppose you know that for a particular number x,

$$x - 3 = 0 \quad \text{or} \quad x + 2 = 0.$$

If you also know that x is not negative, then $x \neq -2$, so

$$x + 2 \neq 0.$$

By elimination, you can then conclude that

$$\therefore x - 3 = 0.$$

■

Example 2.3.6 **Transitivity**

The following argument form is valid:

$$\begin{aligned} p &\to q \\ q &\to r \\ \therefore\ p &\to r \end{aligned}$$

Many arguments in mathematics contain chains of if-then statements. From the fact that one statement implies a second and the second implies a third, you can conclude that the first statement implies the third. In the example below suppose n is a particular integer.

If n is divisible by 18, then n is divisible by 9.
If n is divisible by 9, then the sum of the digits of n is divisible by 9.
$\therefore$ If n is divisible by 18, then the sum of the digits of n is divisible by 9. ■

Example 2.3.7 **Proof by Division into Cases**

The following argument form is valid:

$$\begin{aligned} p &\vee q \\ p &\to r \\ q &\to r \\ \therefore\ r & \end{aligned}$$

It often happens that you know one thing or another is true. If you can show that in either case a certain conclusion follows, then this conclusion must also be true. For instance, suppose you know that x is a particular nonzero real number that is not zero. The trichotomy property of the real numbers says that any real number is positive, negative, or zero. Thus (by elimination) you know that x is positive or x is negative. You can deduce that $x^2 > 0$ by arguing as follows:

x is positive or x is negative.
If x is positive, then $x^2 > 0$.
If x is negative, then $x^2 > 0$.
$\therefore x^2 > 0$. ■

The rules of valid inference are used constantly in problem solving. Here is an example from everyday life.

Example 2.3.8 **Application: A More Complex Deduction**

You are about to leave for class in the morning and discover that you don't have your glasses. You know the following statements are true:

a. If I was reading my class notes in the kitchen, then my glasses are on the kitchen table.
b. If my glasses are on the kitchen table, then I saw them at breakfast.
c. I did not see my glasses at breakfast.
d. I was reading my class notes in the living room or I was reading my class notes in the kitchen.
e. If I was reading my class notes in the living room then my glasses are on the coffee table.

Where are the glasses?

Solution Let RK = I was reading my class notes in the kitchen.
GK = My glasses are on the kitchen table.
SB = I saw my glasses at breakfast.
RL = I was reading my class notes in the living room.
GC = My glasses are on the coffee table.

Here is a sequence of steps you might use to reach the answer, together with the rules of inference that allow you to draw the conclusion of each step:

1.	$RK \rightarrow GK$	by (a)
	$GK \rightarrow SB$	by (b)
	$\therefore RK \rightarrow SB$	by transitivity
2.	$RK \rightarrow SB$	by the conclusion of (1)
	$\sim SB$	by (c)
	$\therefore \sim RK$	by modus tollens
3.	$RL \vee RK$	by (d)
	$\sim RK$	by the conclusion of (2)
	$\therefore RL$	by elimination
4.	$RL \rightarrow GC$	by (e)
	RL	by the conclusion of (3)
	$\therefore GC$	by modus ponens

Thus the glasses are on the coffee table. ■

Fallacies

A **fallacy** is an error in reasoning that results in an invalid argument. Three common fallacies are **using ambiguous premises**, and treating them as if they were unambiguous, **circular reasoning** (**assuming what is to be proved** without having derived it from the premises), and **jumping to a conclusion** (without adequate grounds). In this section we discuss two other fallacies, called *converse error* and *inverse error*, which give rise to arguments that superficially resemble those that are valid by modus ponens and modus tollens but are not, in fact, valid.

As in previous examples, you can show that an argument is invalid by constructing a truth table for the argument form and finding at least one critical row in which all the premises are true but the conclusion is false. Another way is to find an argument of the same form with true premises and a false conclusion.

For an argument to be valid, every argument of the same form whose premises are all true must have a true conclusion. It follows that for an argument to be invalid means that there is an argument of that form whose premises are all true and whose conclusion is false.

Example 2.3.9 **Converse Error**

Show that the following argument is invalid:

If Zeke is a cheater, then Zeke sits in the back row.
Zeke sits in the back row.
$\therefore$ Zeke is a cheater.

Solution Many people recognize the invalidity of the above argument intuitively, reasoning something like this: The first premise gives information about Zeke *if* it is known he is a cheater. It doesn't give any information about him if it is not already known that he is a cheater. One can certainly imagine a person who is not a cheater but happens to sit in the back row. Then if that person's name is substituted for Zeke, the first premise is true by default and the second premise is also true but the conclusion is false.

The general form of the previous argument is as follows:

$$\begin{array}{l} p \rightarrow q \\ q \\ \therefore p \end{array}$$

In exercise 12(a) at the end of this section you are asked to use a truth table to show that this form of argument is invalid. ■

The fallacy underlying this invalid argument form is called the **converse error** because the conclusion of the argument would follow from the premises if the premise $p \rightarrow q$ were replaced by its converse. Such a replacement is not allowed, however, because a conditional statement is not logically equivalent to its converse. Converse error is also known as the *fallacy of affirming the consequent*.

A related common reasoning error is shown in the next example.

Example 2.3.10 **Inverse Error**

Consider the following argument:

If these two vertices are adjacent, then they do not have the same color.
These two vertices are not adjacent.
$\therefore$ These two vertices have the same color.

Note that this argument has the following form:

$$\begin{array}{l} p \rightarrow q \\ \sim p \\ \therefore \sim q \end{array}$$

Caution! In logic, the words *true* and *valid* have very different meanings. A valid argument may have a false conclusion, and an invalid argument may have a true conclusion.

You are asked to give a truth table verification of the invalidity of this argument form in exercise 12(b) at the end of this section.

The fallacy underlying this invalid argument form is called the **inverse error** because the conclusion of the argument would follow from the premises if the premise $p \rightarrow q$ were replaced by its inverse. Such a replacement is not allowed, however, because a conditional statement is not logically equivalent to its inverse. Inverse error is also known as the *fallacy of denying the antecedent*. ■

Sometimes people lump together the ideas of validity and truth. If an argument seems valid, they accept the conclusion as true. And if an argument seems fishy (really a slang expression for invalid), they think the conclusion must be false. This is not correct!

Example 2.3.11 **A Valid Argument with a False Premise and a False Conclusion**

The argument below is valid by modus ponens. But its major premise is false, and so is its conclusion.

If Canada is north of the United States, then temperatures in Canada never rise above freezing.

Canada is north of the United States.

∴ Temperatures in Canada never rise above freezing. ■

Example 2.3.12 **An Invalid Argument with True Premises and a True Conclusion**

The argument below is invalid by the converse error, but it has a true conclusion.

If New York is a big city, then New York has tall buildings.

New York has tall buildings.

∴ New York is a big city. ■

Definition

An argument is called **sound** if, and only if, it is valid *and* all its premises are true. An argument that is not sound is called **unsound**.

The important thing to note is that validity is a property of argument *forms:* If an argument is valid, then so is every other argument that has the same form. Similarly, if an argument is invalid, then so is every other argument that has the same form. What characterizes a valid argument is that no argument whose form is valid can have all true premises and a false conclusion. For each valid argument, there are arguments of that form with all true premises and a true conclusion, with at least one false premise and a true conclusion, and with at least one false premise and a false conclusion. On the other hand, for each invalid argument, there are arguments of that form with every combination of truth values for the premises and conclusion, including all true premises and a false conclusion. The bottom line is that we can only be sure that the conclusion of an argument is true when we know that the argument is sound, that is, when we know both that the argument is valid and that it has all true premises.

Contradictions and Valid Arguments

The concept of logical contradiction can be used to make inferences through a technique of reasoning called the *contradiction rule*. Suppose p is some statement whose truth you wish to deduce.

Contradiction Rule

If you can show that the supposition that statement p is false leads logically to a contradiction, then you can conclude that p is true.

Example 2.3.13 **Contradiction Rule**

Show that the following argument form is valid:

$\sim p \rightarrow \mathbf{c}$, where $\mathbf{c}$ is a contradiction

$\therefore p$

Solution Construct a truth table for the premise and the conclusion of this argument.

			premises	conclusion
p	$\sim p$	$\mathbf{c}$	$\sim p \rightarrow \mathbf{c}$	p
T	F	F	T	T
F	T	F	F	

There is only one critical row in which the premise is true, and in this row the conclusion is also true. Hence this form of argument is valid. ■

The contradiction rule is the logical heart of the method of proof by contradiction. A slight variation also provides the basis for solving many logical puzzles by eliminating contradictory answers: *If an assumption leads to a contradiction, then that assumption must be false.*

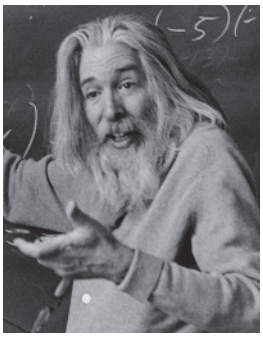
Example 2.3.14 **Knights and Knaves**

The logician Raymond Smullyan describes an island containing two types of people: knights who always tell the truth and knaves who always lie.* You visit the island and are approached by two natives who speak to you as follows:

A says: *B* is a knight.

B says: *A* and I are of opposite type.

What are *A* and *B*?



Eddie Hausner/The *New York Times*/Redux

Raymond Smullyan (1919–2017)

Solution *A* and *B* are both knaves. To see this, reason as follows:

Suppose *A* is a knight.

$\therefore$ What *A* says is true. by definition of knight

$\therefore$ *B* is also a knight. That's what *A* said.

$\therefore$ What *B* says is true. by definition of knight

$\therefore$ *A* and *B* are of opposite types. That's what *B* said.

$\therefore$ We have arrived at the following contradiction: *A* and *B* are both knights and *A* and *B* are of opposite type.

$\therefore$ The supposition is false. by the contradiction rule

$\therefore$ *A* is not a knight. negation of supposition

$\therefore$ *A* is a knave. by elimination: It's given that all inhabitants are knights or knaves, so since *A* is not a knight, *A* is a knave.

$\therefore$ What *A* says is false.

$\therefore$ *B* is not a knight.

$\therefore$ *B* is also a knave. by elimination

*Raymond Smullyan has written a delightful series of whimsical yet profound books of logical puzzles starting with *What Is the Name of This Book?* (Englewood Cliffs, New Jersey: Prentice-Hall, 1978). Other good sources of logical puzzles are the many excellent books of Martin Gardner, such as *Aha! Insight* and *Aha! Gotcha* (New York: W. H. Freeman, 1978, 1982).

This reasoning shows that if the problem has a solution at all, then A and B must both be knaves. It is conceivable, however, that the problem has no solution. The problem statement could be inherently contradictory. If you look back at the solution, though, you can see that it does work out for both A and B to be knaves. ■

Summary of Rules of Inference

Table 2.3.1 summarizes some of the most important rules of inference.

TABLE 2.3.1 Valid Argument Forms

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \to \mathbf{c}$ $\therefore p$

TEST YOURSELF

1. For an argument to be valid means that every argument of the same form whose premises _____ has a _____ conclusion.
2. For an argument to be invalid means that there is an argument of the same form whose premises _____ and whose conclusion _____.
3. For an argument to be sound means that it is _____ and its premises _____. In this case we can be sure that its conclusion _____.

EXERCISE SET 2.3

Use modus ponens or modus tollens to fill in the blanks in the arguments of 1–5 so as to produce valid inferences.

1. If $\sqrt{2}$ is rational, then $\sqrt{2} = a/b$ for some integers a and b.
   It is not true that $\sqrt{2} = a/b$ for some integers a and b.
   $\therefore$ _____.
2. If $1 - 0.99999\ldots$ is less than every positive real number, then it equals zero.
   _____.
   $\therefore$ The number $1 - 0.99999\ldots$ equals zero.
3. If logic is easy, then I am a monkey's uncle.
   I am not a monkey's uncle.
   $\therefore$ _____.
4. If this graph can be colored with three colors, then it can colored with four colors.
   This graph cannot be colored with four colors.
   $\therefore$ _____.
5. If they were unsure of the address, then they would have telephoned.
   _____.
   $\therefore$ They were sure of the address.

Use truth tables to determine whether the argument forms in 6–11 are valid. Indicate which columns represent the premises and which represent the conclusion, and include a sentence explaining how the truth table supports your answer. Your explanation should show that you understand what it means for a form of argument to be valid or invalid.

6. $p \to q$
$q \to p$
$\therefore p \vee q$

7. p
$p \to q$
$\sim q \vee r$
$\therefore r$

8. $p \vee q$
$p \to \sim q$
$p \to r$
$\therefore r$

9. $p \wedge q \to \sim r$
$p \vee \sim q$
$\sim q \to p$
$\therefore \sim r$

10. $p \vee q \to r$
$\therefore \sim r \to \sim p \wedge \sim q$
(This is the form of argument shown on pages 37 and 38.)

11. $p \to q \vee r$
$\sim q \vee \sim r$
$\therefore \sim p \vee \sim r$

12. Use truth tables to show that the following forms of argument are invalid.

a. $p \to q$
q
$\therefore p$
(converse error)

b. $p \to q$
$\sim p$
$\therefore \sim q$
(inverse error)

Use truth tables to show that the argument forms referred to in 13–21 are valid. Indicate which columns represent the premises and which represent the conclusion, and include a sentence explaining how the truth table supports your answer. Your explanation should show that you understand what it means for a form of argument to be valid.

13. Modus tollens:
$p \to q$
$\sim q$
$\therefore \sim p$

14. Example 2.3.3(a)

15. Example 2.3.3(b)

16. Example 2.3.4(a)

17. Example 2.3.4(b)

18. Example 2.3.5(a)

19. Example 2.3.5(b)

20. Example 2.3.6

21. Example 2.3.7

Use symbols to write the logical form of each argument in 22 and 23, and then use a truth table to test the argument for validity. Indicate which columns represent the premises and which represent the conclusion, and include a few words of explanation showing that you understand the meaning of validity.

22. If Tom is not on team A, then Hua is on team B.
If Hua is not on team B, then Tom is on team A.
$\therefore$ Tom is not on team A or Hua is not on team B.

23. Oleg is a math major or Oleg is an economics major.
If Oleg is a math major, then Oleg is required to take Math 362.
$\therefore$ Oleg is an economics major or Oleg is not required to take Math 362.

Some of the arguments in 24–32 are valid, whereas others exhibit the converse or the inverse error. Use symbols to write the logical form of each argument. If the argument is valid, identify the rule of inference that guarantees its validity. Otherwise, state whether the converse or the inverse error is made.

24. If Jules solved this problem correctly, then Jules obtained the answer 2.
Jules obtained the answer 2.
$\therefore$ Jules solved this problem correctly.

25. This real number is rational or it is irrational.
This real number is not rational.
$\therefore$ This real number is irrational.

26. If I go to the movies, I won't finish my homework.
If I don't finish my homework, I won't do well on the exam tomorrow.
$\therefore$ If I go to the movies, I won't do well on the exam tomorrow.

27. If this number is larger than 2, then its square is larger than 4.
This number is not larger than 2.
$\therefore$ The square of this number is not larger than 4.

28. If there are as many rational numbers as there are irrational numbers, then the set of all irrational numbers is infinite.
The set of all irrational numbers is infinite.
$\therefore$ There are as many rational numbers as there are irrational numbers.

29. If at least one of these two numbers is divisible by 6, then the product of these two numbers is divisible by 6.
Neither of these two numbers is divisible by 6.
$\therefore$ The product of these two numbers is not divisible by 6.

30. If this computer program is correct, then it produces the correct output when run with the test data my teacher gave me.
This computer program produces the correct output when run with the test data my teacher gave me.
∴ This computer program is correct.

31. Sandra knows Java and Sandra knows C++.
∴ Sandra knows C++.

32. If I get a Christmas bonus, I'll buy a stereo.
If I sell my motorcycle, I'll buy a stereo.
∴ If I get a Christmas bonus or I sell my motorcycle, then I'll buy a stereo.

33. Give an example (other than Example 2.3.11) of a valid argument with a false conclusion.

34. Give an example (other than Example 2.3.12) of an invalid argument with a true conclusion.

35. Explain in your own words what distinguishes a valid form of argument from an invalid one.

36. Given the following information about a computer program, find the mistake in the program.
- **a.** There is an undeclared variable or there is a syntax error in the first five lines.
- **b.** If there is a syntax error in the first five lines, then there is a missing semicolon or a variable name is misspelled.
- **c.** There is not a missing semicolon.
- **d.** There is not a misspelled variable name.

37. In the back of an old cupboard you discover a note signed by a pirate famous for his bizarre sense of humor and love of logical puzzles. In the note he wrote that he had hidden treasure somewhere on the property. He listed five true statements (a–e below) and challenged the reader to use them to figure out the location of the treasure.
- **a.** If this house is next to a lake, then the treasure is not in the kitchen.
- **b.** If the tree in the front yard is an elm, then the treasure is in the kitchen.
- **c.** This house is next to a lake.
- **d.** The tree in the front yard is an elm or the treasure is buried under the flagpole.
- **e.** If the tree in the back yard is an oak, then the treasure is in the garage.

Where is the treasure hidden?

38. You are visiting the island described in Example 2.3.14 and have the following encounters with natives.
- **a.** Two natives A and B address you as follows:
A says: Both of us are knights.
B says: A is a knave.
What are A and B?
- **b.** Another two natives C and D approach you but only C speaks.
C says: Both of us are knaves.
What are C and D?
- **c.** You then encounter natives E and F.
E says: F is a knave.
F says: E is a knave.
How many knaves are there?
- ***H*** **d.** Finally, you meet a group of six natives, U, V, W, X, Y, and Z, who speak to you as follows:
U says: None of us is a knight.
V says: At least three of us are knights.
W says: At most three of us are knights.
X says: Exactly five of us are knights.
Y says: Exactly two of us are knights.
Z says: Exactly one of us is a knight.
Which are knights and which are knaves?

39. The famous detective Percule Hoirot was called in to solve a baffling murder mystery. He determined the following facts:
- **a.** Lord Hazelton, the murdered man, was killed by a blow on the head with a brass candlestick.
- **b.** Either Lady Hazelton or a maid, Sara, was in the dining room at the time of the murder.
- **c.** If the cook was in the kitchen at the time of the murder, then the butler killed Lord Hazelton with a fatal dose of strychnine.
- **d.** If Lady Hazelton was in the dining room at the time of the murder, then the chauffeur killed Lord Hazelton.
- **e.** If the cook was not in the kitchen at the time of the murder, then Sara was not in the dining room when the murder was committed.
- **f.** If Sara was in the dining room at the time the murder was committed, then the wine steward killed Lord Hazelton.

Is it possible for the detective to deduce the identity of the murderer from these facts? If so, who did murder Lord Hazelton? (Assume there was only one cause of death.)

40. Sharky, a leader of the underworld, was killed by one of his own band of four henchmen. Detective Sharp interviewed the men and determined that all were lying except for one. He deduced who killed Sharky on the basis of the following statements:
- **a.** Socko: Lefty killed Sharky.
- **b.** Fats: Muscles didn't kill Sharky.

c. Lefty: Muscles was shooting craps with Socko when Sharky was knocked off.
d. Muscles: Lefty didn't kill Sharky.
Who did kill Sharky?

In 41–44 a set of premises and a conclusion are given. Use the valid argument forms listed in Table 2.3.1 to deduce the conclusion from the premises, giving a reason for each step as in Example 2.3.8. Assume all variables are statement variables.

41. **a.** $\sim p \vee q \rightarrow r$
b. $s \vee \sim q$
c. $\sim t$
d. $p \rightarrow t$
e. $\sim p \wedge r \rightarrow \sim s$
f. $\therefore \sim q$

42. **a.** $p \vee q$
b. $q \rightarrow r$
c. $p \wedge s \rightarrow t$
d. $\sim r$
e. $\sim q \rightarrow u \wedge s$
f. $\therefore t$

43. **a.** $\sim p \rightarrow r \wedge \sim s$
b. $t \rightarrow s$
c. $u \rightarrow \sim p$
d. $\sim w$
e. $u \vee w$
f. $\therefore \sim t$

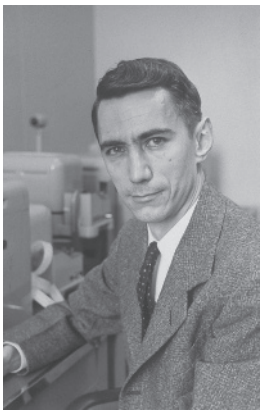
44. **a.** $p \rightarrow q$
b. $r \vee s$
c. $\sim s \rightarrow \sim t$
d. $\sim q \vee s$
e. $\sim s$
f. $\sim p \wedge r \rightarrow u$
g. $w \vee t$
h. $\therefore u \wedge w$

ANSWERS FOR TEST YOURSELF

1. are all true; true **2.** are all true; is false **3.** valid; are all true; is true

2.4 Application: Digital Logic Circuits

Only connect! —E. M. Forster, *Howards End*



Alfred Eisenstaedt/Getty Images

Claude Shannon (1916–2001)

In the late 1930s, a young M.I.T. graduate student named Claude Shannon noticed an analogy between the operations of switching devices, such as telephone switching circuits, and the operations of logical connectives. He used this analogy with striking success to solve problems of circuit design and wrote up his results in his master's thesis, which was published in 1938.

The drawing in Figure 2.4.1(a) shows the appearance of the two positions of a simple switch. When the switch is closed, current can flow from one terminal to the other; when it is open, current cannot flow. Imagine that such a switch is part of the circuit shown in Figure 2.4.1(b). The light bulb turns on if, and only if, current flows through it. And this happens if, and only if, the switch is closed.

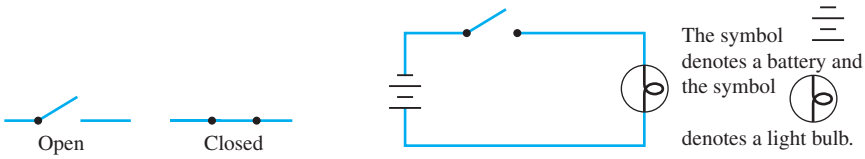


FIGURE 2.4.1

Now consider the more complicated circuits of Figures 2.4.2(a) and 2.4.2(b).

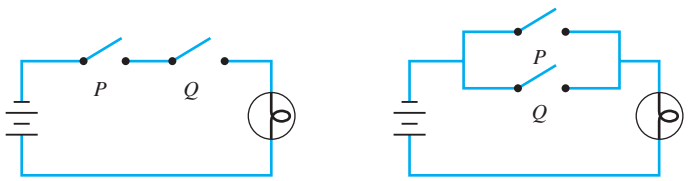


FIGURE 2.4.2

In the circuit of Figure 2.4.2(a) current flows and the light bulb turns on if, and only if, *both* switches P and Q are closed. The switches in this circuit are said to be **in series**. In the circuit of Figure 2.4.2(b) current flows and the light bulb turns on if, and only if, *at least one* of the switches P or Q is closed. The switches in this circuit are said to be **in parallel**. All possible behaviors of these circuits are described by Table 2.4.1.

TABLE 2.4.1

(a) Switches in Series

Switches		Light Bulb
P	Q	State
closed	closed	on
closed	open	off
open	closed	off
open	open	off

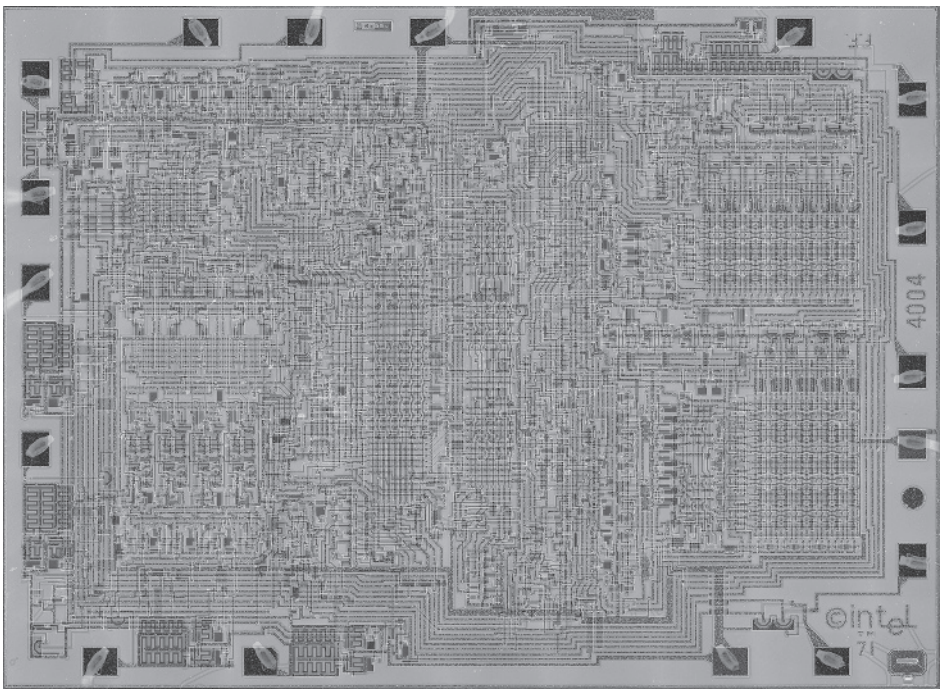
(b) Switches in Parallel

Switches		Light Bulb
P	Q	State
closed	closed	on
closed	open	on
open	closed	on
open	open	off

Observe that if the words *closed* and *on* are replaced by T and *open* and *off* are replaced by F, Table 2.4.1(a) becomes the truth table for *and* and Table 2.4.1(b) becomes the truth table for *or*. Consequently, the switching circuit of Figure 2.4.2(a) is said to correspond to the logical expression $P \wedge Q$, and that of Figure 2.4.2(b) is said to correspond to $P \vee Q$.

More complicated circuits correspond to more complicated logical expressions. This correspondence has been used extensively in the design and study of circuits.

In the 1940s and 1950s, switches were replaced by electronic devices, with the physical states of closed and open corresponding to electronic states such as high and low voltages.



Tim McNerney

The Intel 4004, introduced in 1971, is generally considered to be the first commercially viable microprocessor or central processing unit (CPU) contained on a chip about the size of a fingernail. It consisted of 2,300 transistors and could execute 70,000 instructions per second, essentially the same computing power as the first electronic computer, the ENIAC, built in 1946, which filled an entire room. Modern microprocessors consist of several CPUs on one chip, contain close to a billion transistors and many hundreds of millions of logic circuits, and can compute hundreds of millions of instructions per second.

Alfred Eisenstaedt/Time Life Pictures/Getty Images

John W. Tukey (1915–2000)

The new electronic technology led to the development of modern digital systems such as electronic computers, electronic telephone switching systems, traffic light controls, electronic calculators, and the control mechanisms used in hundreds of other types of electronic equipment. The basic electronic components of a digital system are called *digital logic circuits*. The word *logic* indicates the important role of logic in the design of such circuits, and the word *digital* indicates that the circuits process discrete, or separate, signals as opposed to continuous ones.

Electrical engineers continue to use the language of logic when they refer to values of signals produced by an electronic switch as being "true" or "false." But they generally use the symbols 1 and 0 rather than T and F to denote these values. The symbols 0 and 1 are called **bits**, short for *b*inary dig*its*. This terminology was introduced in 1946 by the statistician John Tukey.

Black Boxes and Gates

Combinations of signal bits (1's and 0's) can be transformed into other combinations of signal bits (1's and 0's) by means of various circuits. Because a variety of different technologies are used in circuit construction, computer engineers and digital system designers find it useful to think of certain basic circuits as black boxes. The inside of a black box contains the detailed implementation of the circuit and is often ignored while attention is focused on the relation between the **input** and the **output** signals.

The operation of a black box is completely specified by constructing an **input/output table** that lists all its possible input signals together with their corresponding output signals. For example, the black box pictured above has three input signals. Since each of these signals can take the value 1 or 0, there are eight possible combinations of input signals. One possible correspondence of input to output signals is as follows:

An Input/Output Table

Input			Output
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

The third row, for instance, indicates that for inputs $P = 1$, $Q = 0$, and $R = 1$, the output S is 0.

An efficient method for designing more complicated circuits is to build them by connecting less complicated black box circuits. Three such circuits are known as NOT-, AND-, and OR-gates.

A **NOT-gate** (or **inverter**) is a circuit with one input signal and one output signal. If the input signal is 1, the output signal is 0. Conversely, if the input signal is 0, then the output signal is 1. An **AND-gate** is a circuit with two input signals and one output signal. If both input signals are 1, then the output signal is 1. Otherwise, the output signal is 0. An **OR-gate** also has two input signals and one output signal. If both input signals are 0, then the output signal is 0. Otherwise, the output signal is 1.

The actions of NOT-, AND-, and OR-gates are summarized in Figure 2.4.3, where P and Q represent input signals and R represents the output signal. It should be clear from Figure 2.4.3 that the actions of the NOT-, AND-, and OR-gates on signals correspond exactly to those of the logical connectives $\sim$, $\wedge$, and $\vee$ on statements, if the symbol 1 is identified with T and the symbol 0 is identified with F.

Gates can be combined into circuits in a variety of ways. If the rules shown at the bottom of the page are obeyed, the result is a **combinational circuit**, one whose output at any time is determined entirely by its input at that time without regard to previous inputs.

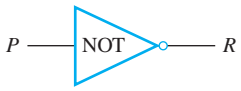
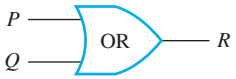
<table>
<tr><th>Type of Gate</th><th>Symbolic Representation</th><th>Action</th></tr>
<tr><td>NOT</td><td> 
</td><td>
<table>
<tr><th>Input</th><th>Output</th></tr>
<tr><th>P</th><th>R</th></tr>
<tr><td>1</td><td>0</td></tr>
<tr><td>0</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>AND</td><td> 
</td><td>
<table>
<tr><th colspan="2">Input</th><th>Output</th></tr>
<tr><th>P</th><th>Q</th><th>R</th></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
</table>
</td></tr>
<tr><td>OR</td><td> 
</td><td>
<table>
<tr><th colspan="2">Input</th><th>Output</th></tr>
<tr><th>P</th><th>Q</th><th>R</th></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>0</td><td>1</td><td>1</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
</table>
</td></tr>
</table>

FIGURE 2.4.3

Rules for a Combinational Circuit

Never combine two input wires. 2.4.1
A single input wire can be split partway and used as input for two separate gates. 2.4.2
An output wire can be used as input. 2.4.3
No output of a gate can eventually feed back into that gate. 2.4.4

Rule (2.4.4) is violated in more complex circuits, called **sequential circuits**, whose output at any given time depends both on the input at that time and also on previous inputs. These circuits are discussed in Section 12.2.

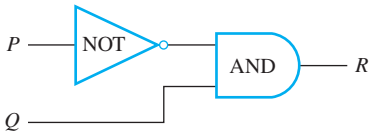
The Input/Output Table for a Circuit

If you are given a set of input signals for a circuit, you can find its output by tracing through the circuit gate by gate.

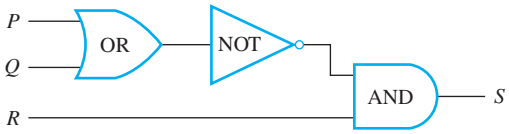
Example 2.4.1 **Determining Output for a Given Input**

Indicate the output of the circuits shown below for the given input signals.

a. Input signals: $P = 0$ and $Q = 1$

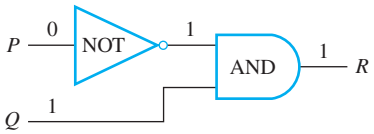


b. Input signals: $P = 1$, $Q = 0$, $R = 1$

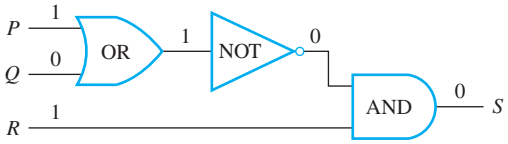


Solution

a. Move from left to right through the diagram, tracing the action of each gate on the input signals. The NOT-gate changes $P = 0$ to a 1, so both inputs to the AND-gate are 1; hence the output R is 1. This is illustrated by annotating the diagram as shown below.



b. The output of the OR-gate is 1 since one of the input signals, P, is 1. The NOT-gate changes this 1 into a 0, so the two inputs to the AND-gate are 0 and $R = 1$. Hence the output S is 0. The trace is shown below.

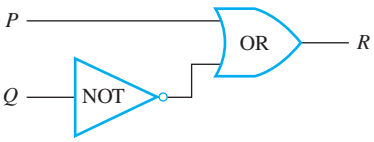


■

To construct the entire input/output table for a circuit, trace through the circuit to find the corresponding output signals for each possible combination of input signals.

Example 2.4.2 **Constructing the Input/Output Table for a Circuit**

Construct the input/output table for the following circuit.



Illustrated London News Ltd./ Pantheon/Superstock

George Boole (1815–1864)

Solution List the four possible combinations of input signals, and find the output for each by tracing through the circuit.

Input		Output
P	***Q***	***R***
1	1	1
1	0	1
0	1	0
0	0	1

■

The Boolean Expression Corresponding to a Circuit

In logic, variables such as p, q, and r represent statements, and a statement can have one of only two truth values: T (true) or F (false). A statement form is an expression, such as $p \wedge (\sim q \vee r)$, composed of statement variables and logical connectives.

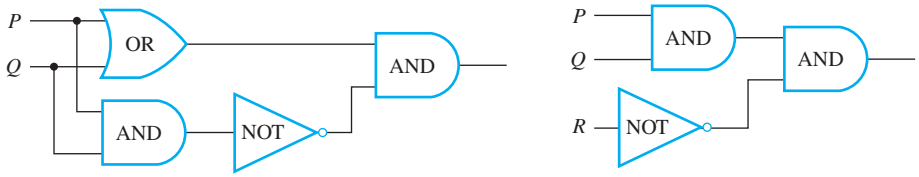
As noted earlier, one of the founders of symbolic logic was the English mathematician George Boole. In his honor, any variable, such as a statement variable or an input signal, that can take one of only two values is called a **Boolean variable**. An expression composed of Boolean variables and the connectives $\sim$, $\wedge$, and $\vee$ is called a **Boolean expression**.

Given a circuit consisting of combined NOT-, AND-, and OR-gates, a corresponding Boolean expression can be obtained by tracing the actions of the gates on the input variables.

Note Strictly speaking, only meaningful expressions such as $(\sim p \wedge q) \vee (p \wedge r)$ and $\sim(\sim(p \wedge q) \vee r)$ are allowed as Boolean, not meaningless ones like $p \sim q((rs \vee \ \wedge q\sim$. We use recursion to give a careful definition of Boolean expressions in Section 5.9.

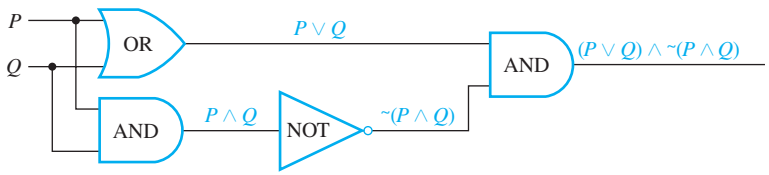
Example 2.4.3 **Finding a Boolean Expression for a Circuit**

Find the Boolean expressions that correspond to the circuits shown below. A black dot indicates a soldering of two wires; wires that cross without a dot are assumed not to touch.



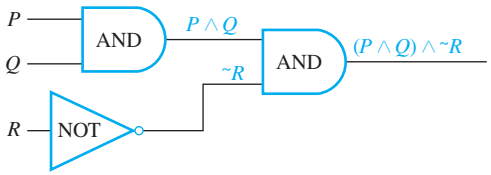
Solution

a. Trace through the circuit from left to right, indicating the output of each gate symbolically, as shown below.



The final expression obtained, $(P \vee Q) \wedge \sim(P \wedge Q)$, is the expression for exclusive or: P or Q but not both.

b. The Boolean expression corresponding to the circuit is $(P \wedge Q) \wedge \sim R$, as shown on the next page.



Observe that the output of the circuit shown in Example 2.4.3(b) is 1 for exactly one combination of inputs ($P = 1$, $Q = 1$, and $R = 0$) and is 0 for all other combinations of inputs. For this reason, the circuit can be said to "recognize" one particular combination of inputs. The output column of the input/output table has a 1 in exactly one row and 0's in all other rows.

Definition

A **recognizer** is a circuit that outputs a 1 for exactly one particular combination of input signals and outputs 0's for all other combinations.

Input/Output Table for a Recognizer

P	Q	R	$(P \wedge Q) \wedge \sim R$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

The Circuit Corresponding to a Boolean Expression

The preceding examples showed how to find a Boolean expression corresponding to a circuit. The following example shows how to construct a circuit corresponding to a Boolean expression. The strategy is to work from the outermost part of the Boolean expression to the innermost part, adding logic gates that correspond to the operations in the expression as you move from right to left in the circuit diagram.

Example 2.4.4 **Constructing Circuits for Boolean Expressions**

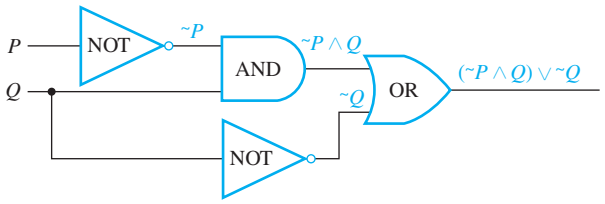
Construct circuits for the following Boolean expressions.

a. $(\sim P \wedge Q) \vee \sim Q$ b. $((P \wedge Q) \wedge (R \wedge S)) \wedge T$

Solution

a. Write the input variables in a column on the left side of the diagram. Since the last operation executed when evaluating $(\sim P \wedge Q) \vee \sim Q$ is $\vee$, put an OR-gate at the extreme

right of the diagram. One input to this gate is $\sim P \wedge Q$, so draw an AND-gate to the left of the OR-gate and show its output coming into the OR-gate. Since one input to the AND-gate is $\sim P$, draw a line from P to a NOT-gate and from there to the AND-gate. Since the other input to the AND-gate is Q, draw a line from Q directly to the AND-gate. The other input to the OR-gate is $\sim Q$, so draw a line from Q to a NOT-gate and from the NOT-gate to the OR-gate. The circuit you obtain is shown below.



b. To start constructing this circuit, put one AND-gate at the extreme right to correspond to the $\wedge$, which is the final operation between $((P \wedge Q) \wedge (R \wedge S))$ and T. To the left of that gate put the AND-gate corresponding to the $\wedge$ between $P \wedge Q$ and $R \wedge S$. To the left of that gate put the two AND-gates corresponding to the $\wedge$'s between P and Q and between R and S. The circuit is shown in Figure 2.4.4.

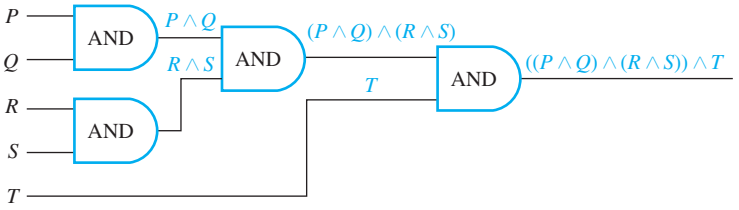


FIGURE 2.4.4 ■

It follows from Theorem 2.1.1 that all the ways of adding parentheses to $P \wedge Q \wedge R \wedge S \wedge T$ give logically equivalent results. Thus, for example,

$$((P \wedge Q) \wedge (R \wedge S)) \wedge T \equiv (P \wedge (Q \wedge R)) \wedge (S \wedge T),$$

and hence the circuit in Figure 2.4.5, which corresponds to $(P \wedge (Q \wedge R)) \wedge (S \wedge T)$, has the same input/output table as the circuit in Figure 2.4.4, which corresponds to $((P \wedge Q) \wedge (R \wedge S)) \wedge T$.

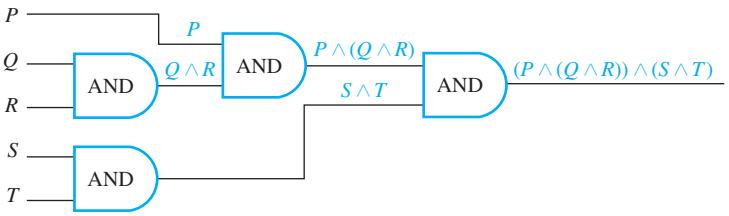


FIGURE 2.4.5

It follows that the circuits in Figures 2.4.4 and 2.4.5 are both implementations of the expression $P \wedge Q \wedge R \wedge S \wedge T$. Such a circuit is called a **multiple-input AND-gate** and is represented by the diagram shown in Figure 2.4.6. **Multiple-input OR-gates** are constructed similarly.

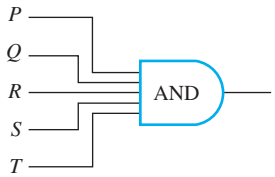


FIGURE 2.4.6

Finding a Circuit That Corresponds to a Given Input/Output Table

To this point, we have discussed how to construct the input/output table for a circuit, how to find the Boolean expression corresponding to a given circuit, and how to construct the circuit corresponding to a given Boolean expression. Now we address the question of how to design a circuit (or find a Boolean expression) corresponding to a given input/output table. The way to do this is to put several recognizers together in parallel.

Example 2.4.5 **Designing a Circuit for a Given Input/Output Table**

Design a circuit for the following input/output table:

Input			Output
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

Solution First construct a Boolean expression with this table as its truth table. To do this, identify each row for which the output is 1—in this case, the rows 1, 3, and 4. For each such row, construct an *and* expression that produces a 1 (or true) for the exact combination of input values for that row and a 0 (or false) for all other combinations of input values.

For example, the expression for row 1 is $\boldsymbol{P \wedge Q \wedge R}$ because $P \wedge Q \wedge R$ is 1 if $P = 1$ and $Q = 1$ and $R = 1$, and it is 0 for all other values of P, Q, and R. The expression for row 3 is $\boldsymbol{P \wedge \sim Q \wedge R}$ because $P \wedge \sim Q \wedge R$ is 1 if $P = 1$ and $Q = 0$ and $R = 1$, and it is 0 for all other values of P, Q, and R. Similarly, the expression for row 4 is $\boldsymbol{P \wedge \sim Q \wedge \sim R}$.

Now any Boolean expression with the given table as its truth table has the value 1 in case $P \wedge Q \wedge R = 1$, or in case $P \wedge \sim Q \wedge R = 1$, or in case $P \wedge \sim Q \wedge \sim R = 1$, and in no other cases. It follows that a Boolean expression with the given truth table is

$$(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R). \qquad 2.4.5$$

The circuit corresponding to this expression has the diagram shown in Figure 2.4.7. Observe that expression (2.4.5) is a disjunction of terms that are themselves conjunctions in

which one of P or $\sim P$, one of Q or $\sim Q$, and one of R or $\sim R$ all appear. Such expressions are said to be in **disjunctive normal form** or **sum-of-products form**.

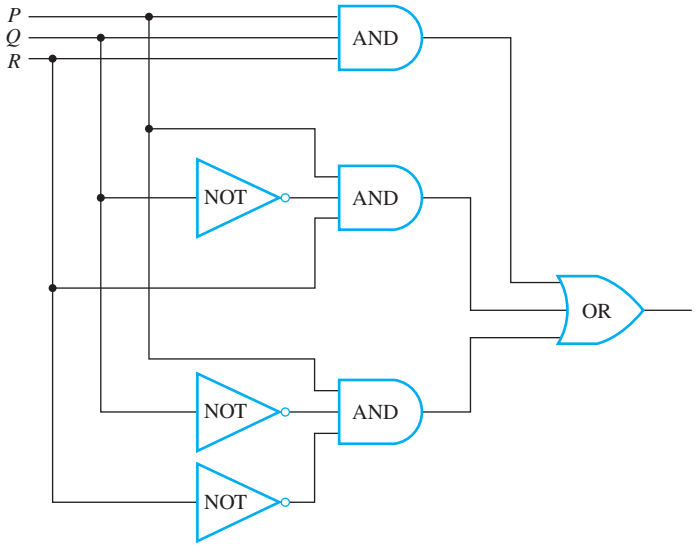
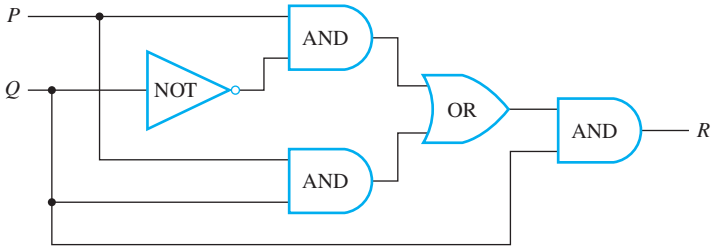


FIGURE 2.4.7

Simplifying Combinational Circuits

Consider the two combinational circuits shown in Figure 2.4.8.



(a)

(b)

FIGURE 2.4.8

If you trace through circuit (a), you will find that its input/output table is

Input		Output
P	***Q***	***R***
1	1	1
1	0	0
0	1	0
0	0	0

which is the same as the input/output table for circuit (b). Thus these two circuits do the same job in the sense that they transform the same combinations of input signals into the same output signals. Yet circuit (b) is simpler than circuit (a) in that it contains many fewer logic gates. Thus, as part of an integrated circuit, it would take less space and require less power.

Definition

Two digital logic circuits are **equivalent** if, and only if, their input/output tables are identical.

Since logically equivalent statement forms have identical truth tables, you can determine that two circuits are equivalent by finding the Boolean expressions corresponding to the circuits and showing that these expressions, regarded as statement forms, are logically equivalent. Example 2.4.6 shows how this procedure works for circuits (a) and (b) in Figure 2.4.8.

Example 2.4.6 **Showing That Two Circuits Are Equivalent**

Find the Boolean expressions for each circuit in Figure 2.4.8. Use Theorem 2.1.1 to show that these expressions are logically equivalent when regarded as statement forms.

Solution The Boolean expressions that correspond to circuits (a) and (b) are $((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q$ and $P \wedge Q$, respectively. By Theorem 2.1.1,

$$\begin{aligned}
&((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q \\
&\quad \equiv (P \wedge (\sim Q \vee Q)) \wedge Q && \text{by the distributive law} \\
&\quad \equiv (P \wedge (Q \vee \sim Q)) \wedge Q && \text{by the commutative law for } \vee \\
&\quad \equiv (P \wedge \mathbf{t}) \wedge Q && \text{by the negation law} \\
&\quad \equiv P \wedge Q && \text{by the identity law.}
\end{aligned}$$

It follows that the truth tables for $((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q$ and $P \wedge Q$ are the same. Hence the input/output tables for the circuits corresponding to these expressions are also the same, and so the circuits are equivalent. ■

In general, you can simplify a combinational circuit by finding the corresponding Boolean expression, using the properties listed in Theorem 2.1.1 to find a Boolean expression that is shorter and logically equivalent to it (when both are regarded as statement forms), and constructing the circuit corresponding to this shorter Boolean expression.

NAND and NOR Gates

HUD 305.25. Harvard University Archives

H. M. Sheffer (1882–1964)

Another way to simplify a circuit is to find an equivalent circuit that uses the least number of different kinds of logic gates. Two gates not previously introduced are particularly useful for this: NAND-gates and NOR-gates. A NAND-gate is a single gate that acts like an AND-gate followed by a NOT-gate. A NOR-gate acts like an OR-gate followed by a NOT-gate. Thus the output signal of a NAND-gate is 0 when, and only when, both input signals are 1, and the output signal for a NOR-gate is 1 when, and only when, both input signals are 0. The logical symbols corresponding to these gates are $|$ (for NAND) and $\downarrow$ (for NOR), where $|$ is called a **Sheffer stroke** (after H. M. Sheffer, 1882–1964) and $\downarrow$ is called a **Peirce arrow** (after C. S. Peirce, 1839–1914; see page 110). Thus

$$P \,|\, Q \equiv \sim(P \wedge Q) \quad \text{and} \quad P \downarrow Q \equiv \sim(P \vee Q).$$

The table below summarizes the actions of NAND and NOR gates.

Type of Gate	Symbolic Representation	Action
NAND		**Input** **P** **Q** / **Output** $R = P \mid Q$: 1 1 → 0; 1 0 → 1; 0 1 → 1; 0 0 → 1
NOR		**Input** **P** **Q** / **Output** $R = P \downarrow Q$: 1 1 → 0; 1 0 → 0; 0 1 → 0; 0 0 → 1

It can be shown that any Boolean expression is equivalent to one written entirely with Sheffer strokes or entirely with Peirce arrows. Thus any digital logic circuit is equivalent to one that uses only NAND-gates or only NOR-gates. Example 2.4.7 develops part of the derivation of this result; the rest is left for the exercises.

Example 2.4.7 **Rewriting Expressions Using the Sheffer Stroke**

Use Theorem 2.1.1 and the definition of Sheffer stroke to show that

a. $\sim P \equiv P|P$ and b. $P \vee Q \equiv (P|P)|(Q|Q)$.

Solution

a. $\sim P \equiv \sim(P \wedge P)$ by the idempotent law for $\wedge$
$\equiv P|P$ by definition of |.

b. $P \vee Q \equiv \sim(\sim(P \vee Q))$ by the double negative law
$\equiv \sim(\sim P \wedge \sim Q)$ by De Morgan's laws
$\equiv \sim((P|P) \wedge (Q|Q))$ by part (a)
$\equiv (P|P)|(Q|Q)$ by definition of |. ■

TEST YOURSELF

1. The input/output table for a digital logic circuit is a table that shows _____.
2. The Boolean expression that corresponds to a digital logic circuit is _____.
3. A recognizer is a digital logic circuit that _____.
4. Two digital logic circuits are equivalent if, and only if, _____.

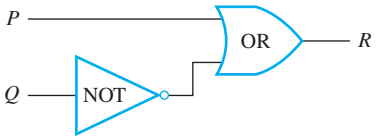
5. A NAND-gate is constructed by placing a _____ gate immediately following an _____ gate.

6. A NOR-gate is constructed by placing a _____ gate immediately following an _____ gate.

EXERCISE SET 2.4

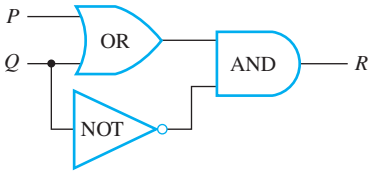
Give the output signals for the circuits in 1–4 if the input signals are as indicated.

1.



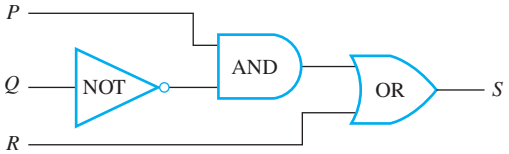
input signals: $P = 1$ and $Q = 1$

2.



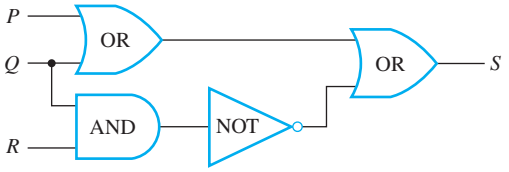
input signals: $P = 1$ and $Q = 0$

3.



input signals: $P = 1$, $Q = 0$, $R = 0$

4.



input signals: $P = 0$, $Q = 0$, $R = 0$

In 5–8, write an input/output table for the circuit in the referenced exercise.

5. Exercise 1 **6.** Exercise 2

7. Exercise 3 **8.** Exercise 4

In 9–12, find the Boolean expression that corresponds to the circuit in the referenced exercise.

9. Exercise 1 **10.** Exercise 2

11. Exercise 3 **12.** Exercise 4

Construct circuits for the Boolean expressions in 13–17.

13. $\sim P \vee Q$ **14.** $\sim(P \vee Q)$

15. $P \vee (\sim P \wedge \sim Q)$ **16.** $(P \wedge Q) \vee \sim R$

17. $(P \wedge \sim Q) \vee (\sim P \wedge R)$

For each of the tables in 18–21, construct (a) a Boolean expression having the given table as its truth table and (b) a circuit having the given table as its input/output table.

18.

P	*Q*	*R*	*S*
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

19.

P	*Q*	*R*	*S*
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

20.

P	*Q*	*R*	*S*
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

21.

P	Q	R	S
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

22. Design a circuit to take input signals P, Q, and R and output a 1 if, and only if, P and Q have the same value and Q and R have opposite values.

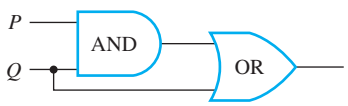
23. Design a circuit to take input signals P, Q, and R and output a 1 if, and only if, all three of P, Q, and R have the same value.

24. The lights in a classroom are controlled by two switches: one at the back of the room and one at the front. Moving either switch to the opposite position turns the lights off if they are on and on if they are off. Assume the lights have been installed so that when both switches are in the down position, the lights are off. Design a circuit to control the switches.

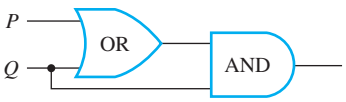
25. An alarm system has three different control panels in three different locations. To enable the system, switches in at least two of the panels must be in the on position. If fewer than two are in the on position, the system is disabled. Design a circuit to control the switches.

Use the properties listed in Theorem 2.1.1 to show that each pair of circuits in 26–29 have the same input/output table. (Find the Boolean expressions for the circuits and show that they are logically equivalent when regarded as statement forms.)

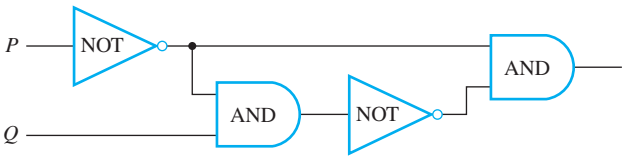
26. a.



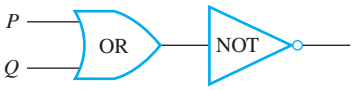
b.



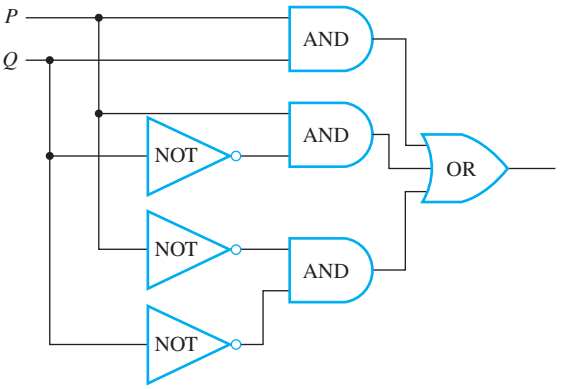
27. a.



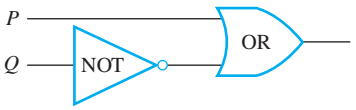
b.



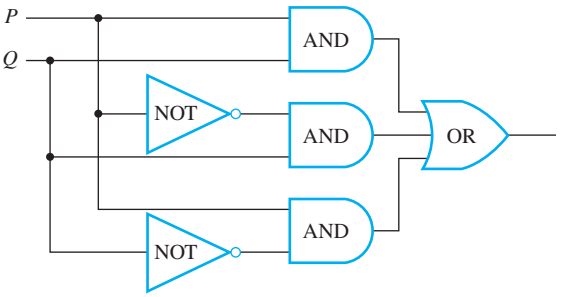
28. a.



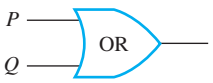
b.



29. a.



b.



For the circuits corresponding to the Boolean expressions in each of 30 and 31 there is an equivalent circuit with at most two logic gates. Find such a circuit.

30. $(P \wedge Q) \vee (\sim P \wedge Q) \vee (\sim P \wedge \sim Q)$

31. $(\sim P \wedge \sim Q) \vee (\sim P \wedge Q) \vee (P \wedge \sim Q)$

32. The Boolean expression for the circuit in Example 2.4.5 is

$$(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R)$$

(a disjunctive normal form). Find a circuit with at most three logic gates that is equivalent to this circuit.

33. a. Show that for the Sheffer stroke $|$,

$$P \wedge Q \equiv (P|Q)|(P|Q).$$

b. Use the results of Example 2.4.7 and part (a) above to write $P \wedge (\sim Q \vee R)$ using only Sheffer strokes.

34. Show that the following logical equivalences hold for the Peirce arrow $\downarrow$, where $P \downarrow Q \equiv \sim(P \vee Q)$.

a. $\sim P \equiv P \downarrow P$

b. $P \vee Q \equiv (P \downarrow Q) \downarrow (P \downarrow Q)$

c. $P \wedge Q \equiv (P \downarrow P) \downarrow (Q \downarrow Q)$

***H* d.** Write $P \rightarrow Q$ using Peirce arrows only.

e. Write $P \leftrightarrow Q$ using Peirce arrows only.

ANSWERS FOR TEST YOURSELF

1. the output signal(s) that correspond to all possible combinations of input signals to the circuit **2.** a Boolean expression that represents the input signals as variables and indicates the successive actions of the logic gates on the input signals **3.** outputs a 1 for exactly one particular combination of input signals and outputs 0's for all other combinations **4.** they have the same input/output table **5.** NOT; AND **6.** NOT; OR

2.5 Application: Number Systems and Circuits for Addition

Counting in binary is just like counting in decimal if you are all thumbs. —Glaser and Way

In elementary school, you learned the meaning of decimal notation: that to interpret a string of decimal digits as a number, you mentally multiply each digit by its place value. For instance, 5,049 has a 5 in the thousands place, a 0 in the hundreds place, a 4 in the tens place, and a 9 in the ones place. Thus

$$5{,}049 = 5 \cdot (1{,}000) + 0 \cdot (100) + 4 \cdot (10) + 9 \cdot (1).$$

Using exponential notation, this equation can be rewritten as

$$5{,}049 = 5 \cdot 10^3 + 0 \cdot 10^2 + 4 \cdot 10^1 + 9 \cdot 10^0.$$

More generally, decimal notation is based on the fact that any positive integer can be written uniquely as a sum of products of the form

$$d \cdot 10^n,$$

where each n is a nonnegative integer and each d is one of the decimal digits 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9. The word *decimal* comes from the Latin root *deci*, meaning "ten." Decimal (or base 10) notation expresses a number as a string of digits in which each digit's position indicates the power of 10 by which it is multiplied. The right-most position is the ones place (or 10^0 place), to the left of that is the tens place (or 10^1 place), to the left of that is the hundreds place (or 10^2 place), and so forth, as illustrated below.

Place	10^3 thousands	10^2 hundreds	10^1 tens	10^0 ones
Decimal Digit	5	0	4	9

Binary Representation of Numbers

There is nothing sacred about the number 10; we use 10 as a base for our usual number system because we happen to have ten fingers. In fact, any integer greater than 1 can serve as a base for a number system. In computer science, **base 2 notation**, or **binary notation**, is of special importance because the signals used in modern electronics are always in one of only two states. (The Latin root *bi* means "two.")

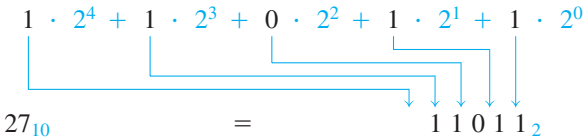
In Section 5.4, we show that any integer can be represented uniquely as a sum of products of the form

$$d \cdot 2^n,$$

where each n is an integer and each d is one of the binary digits (or bits) 0 or 1. For example,

$$\begin{aligned} 27 &= 16 + 8 + 2 + 1 \\ &= 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0. \end{aligned}$$

In binary notation, as in decimal notation, we write just the binary digits, and not the powers of the base. In binary notation, then,



where the subscripts indicate the base, whether 10 or 2, in which the number is written. The places in binary notation correspond to the various powers of 2. The right-most position is the ones place (or 2^0 place), to the left of that is the twos place (or 2^1 place), to the left of that is the fours place (or 2^2 place), and so forth, as illustrated below.

Place	2^4 sixteens	2^3 eights	2^2 fours	2^1 twos	2^0 ones
Binary Digit	1	1	0	1	1

As in the decimal notation, leading zeros may be added or dropped as desired. For example,

$$003_{10} = 3_{10} = 1 \cdot 2^1 + 1 \cdot 2^0 = 11_2 = 011_2.$$

Example 2.5.1 **Binary Notation for Integers from 1 to 9**

Derive the binary notation for the integers from 1 to 9.

Solution

$$\begin{aligned}
1_{10} &= 1 \cdot 2^0 = 1_2 \\
2_{10} &= 1 \cdot 2^1 + 0 \cdot 2^0 = 10_2 \\
3_{10} &= 1 \cdot 2^1 + 1 \cdot 2^0 = 11_2 \\
4_{10} &= 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 100_2 \\
5_{10} &= 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 101_2 \\
6_{10} &= 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 110_2 \\
7_{10} &= 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 111_2 \\
8_{10} &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 1000_2 \\
9_{10} &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1001_2
\end{aligned}$$

■

A list of powers of 2 is useful for doing binary-to-decimal and decimal-to-binary conversions. See Table 2.5.1.

TABLE 2.5.1 Powers of 2

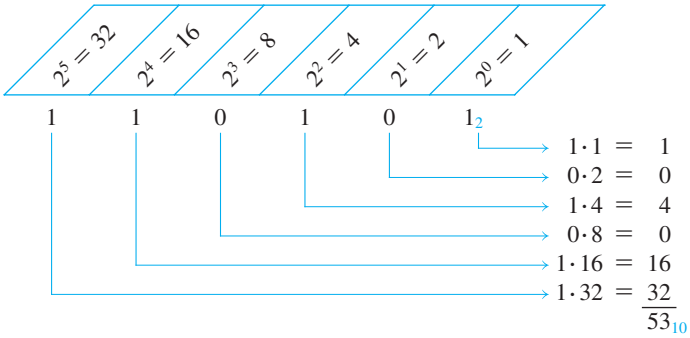
Power of 2	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Form	1024	512	256	128	64	32	16	8	4	2	1

Example 2.5.2 **Converting a Binary to a Decimal Number**

Represent 110101_2 in decimal notation.

Solution
$$\begin{aligned} 110101_2 &= 1\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 \\ &= 32 + 16 + 4 + 1 \\ &= 53_{10} \end{aligned}$$

Alternatively, the schema below may be used.



■

Example 2.5.3 **Converting a Decimal to a Binary Number**

Represent 209 in binary notation.

Solution Use Table 2.5.1 to write 209 as a sum of powers of 2, starting with the highest power of 2 that is less than 209 and continuing to lower powers.

Since 209 is between 128 and 256, the highest power of 2 that is less than 209 is 128. Hence

$$209_{10} = 128 + \text{a smaller number.}$$

Now $209 - 128 = 81$, and 81 is between 64 and 128, so the highest power of 2 that is less than 81 is 64. Hence

$$209_{10} = 128 + 64 + \text{a smaller number.}$$

Continuing in this way, you obtain

$$\begin{aligned} 209_{10} &= 128 + 64 + 16 + 1 \\ &= 1\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0. \end{aligned}$$

For each power of 2 that occurs in the sum, there is a 1 in the corresponding position of the binary number. For each power of 2 that is missing from the sum, there is a 0 in the corresponding position of the binary number. Thus

$$209_{10} = 11010001_2$$

■

Another procedure for converting from decimal to binary notation is discussed in Section 5.1.

Caution! Do not read 10_2 as "ten"; it is the number two. Read 10_2 as "one oh base two."

Binary Addition and Subtraction

The computational methods of binary arithmetic are analogous to those of decimal arithmetic. In binary arithmetic the number 2 (which equals 10_2 in binary notation) plays a role similar to that of the number 10 in decimal arithmetic.

Example 2.5.4 **Addition in Binary Notation**

Add 1101_2 and 111_2 using binary notation.

Solution Because $2_{10} = 10_2$ and $1_{10} = 1_2$, the translation of $1_{10} + 1_{10} = 2_{10}$ to binary notation is

$$\begin{array}{r} 1_2 \\ +\ 1_2 \\ \hline 10_2 \end{array}$$

It follows that adding two 1's together results in a carry of 1 when binary notation is used. Adding three 1's together also results in a carry of 1 since $3_{10} = 11_2$ ("one one base two").

$$\begin{array}{r} 1_2 \\ +\ 1_2 \\ +\ 1_2 \\ \hline 11_2 \end{array}$$

Thus the addition can be performed as follows:

$$\begin{array}{rcccc} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & \\ & 1 & 1 & 0 & 1_2 \\ + & & 1 & 1 & 1_2 \\ \hline 1 & 0 & 1 & 0 & 0_2 \end{array} \quad \leftarrow \text{carry row}$$

■

Example 2.5.5 **Subtraction in Binary Notation**

Subtract 1011_2 from 11000_2 using binary notation.

Solution In decimal subtraction the fact that $10_{10} - 1_{10} = 9_{10}$ is used to borrow across several columns. For example, consider the following:

$$\begin{array}{rcccc} & {\scriptstyle 9} & {\scriptstyle 9} & & \\ & & {\scriptstyle 1} & {\scriptstyle 1} & \leftarrow \text{borrow row} \\ & 1 & 0 & 0 & 0_{10} \\ - & & 5 & 8_{10} & \\ \hline & 9 & 4 & 2_{10} & \end{array}$$

In binary subtraction it may also be necessary to borrow across more than one column. But when you borrow a 1_2 from 10_2, what remains is 1_2.

$$\begin{array}{r} 10_2 \\ -\ 1_2 \\ \hline 1_2 \end{array}$$

Thus the subtraction can be performed as follows:

$$\begin{array}{rcccc} & {\scriptstyle 0} & {\scriptstyle 1} & {\scriptstyle 1} & \\ & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & \leftarrow \text{borrow row} \\ 1 & 1 & 0 & 0 & 0_2 \\ - & 1 & 0 & 1 & 1_2 \\ \hline & 1 & 1 & 0 & 1_2 \end{array}$$

■

Circuits for Computer Addition

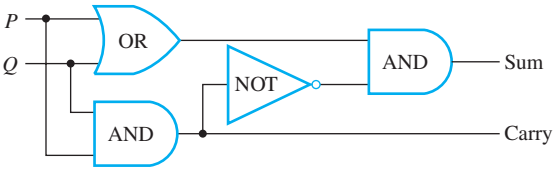
Consider the question of designing a circuit to produce the sum of two binary digits P and Q. Both P and Q can be either 0 or 1. And the following facts are known:

$$\begin{aligned} 1_2 + 1_2 &= 10_2, \\ 1_2 + 0_2 = 1_2 &= 01_2, \\ 0_2 + 1_2 = 1_2 &= 01_2, \\ 0_2 + 0_2 = 0_2 &= 00_2. \end{aligned}$$

It follows that the circuit must have two outputs—one for the left binary digit (this is called the **carry**) and one for the right binary digit (this is called the **sum**). The carry output is 1 if both P and Q are 1; it is 0 otherwise. Thus the carry can be produced using the AND-gate circuit that corresponds to the Boolean expression $P \wedge Q$. The sum output is 1 if either P or Q, but not both, is 1. The sum can, therefore, be produced using a circuit that corresponds to the Boolean expression for *exclusive or*: $(P \vee Q) \wedge \sim(P \wedge Q)$. (See Example 2.4.3(a).) Hence, a circuit to add two binary digits P and Q can be constructed as in Figure 2.5.1. This circuit is called a **half-adder**.

HALF-ADDER

Circuit



Input/OutputTable

P	*Q*	Carry	Sum
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	0

FIGURE 2.5.1 Circuit to Add $P + Q$, Where P and Q Are Binary Digits

Now consider the question of how to construct a circuit to add two binary integers, each with more than one digit. Because the addition of two binary digits may result in a carry to the next column to the left, it may be necessary to add three binary digits at certain points. In the following example, the sum in the right column is the sum of two binary digits, and, because of the carry, the sum in the left column is the sum of three binary digits.

$$\begin{array}{rr} & \overset{1}{} \quad \leftarrow \text{carry row} \\ & 1\ 1_2 \\ + & 1\ 1_2 \\ \hline & 1\ 1\ 0_2 \end{array}$$

Thus, in order to construct a circuit that will add multidigit binary numbers, it is necessary to incorporate a circuit that will compute the sum of three binary digits. Such a circuit is called a **full-adder**. Consider a general addition of three binary digits P, Q, and R that results in a carry (or left-most digit) C and a sum (or right-most digit) S.

$$\begin{array}{r} P \\ + \ Q \\ + \ R \\ \hline CS \end{array}$$

The operation of the full-adder is based on the fact that addition is a binary operation: Only two numbers can be added at one time. Thus P is first added to Q and then the result

is added to R. For instance, consider the following addition:

$$\begin{array}{r} 1_2 \\ +\ 0_2 \\ +\ 1_2 \\ \hline 10_2 \end{array} \quad \left.\begin{array}{l} 1_2 + 0_2 = 01_2 \\ 1_2 + 1_2 = 10_2 \end{array}\right.$$

The process illustrated here can be broken down into steps that use half-adder circuits.

Step 1: Add P and Q using a half-adder to obtain a binary number with two digits.

$$\begin{array}{r} P \\ +\ Q \\ \hline C_1 S_1 \end{array}$$

Step 2: Add R to the sum $C_1\ S_1$ of P and Q.

$$\begin{array}{r} C_1 S_1 \\ +\ R \\ \hline \end{array}$$

To do this, proceed as follows:

Step 2a: Add R to S_1 using a half-adder to obtain the two-digit number $C_2 S$.

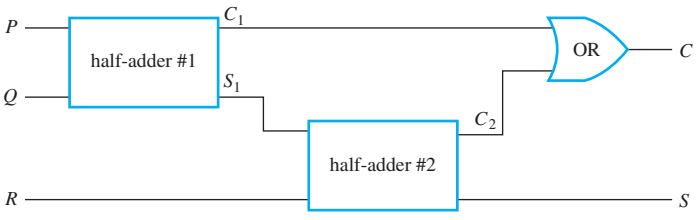
$$\begin{array}{r} S_1 \\ +\ R \\ \hline C_2 S \end{array}$$

Then S is the right-most digit of the entire sum of P, Q, and R.

Step 2b: Determine the left-most digit, C, of the entire sum as follows: First note that it is impossible for both C_1 and C_2 to be 1's. For if $C_1 = 1$, then P and Q are both 1, and so $S_1 = 0$. Consequently, the addition of S_1 and R gives a binary number $C_2 S_1$ where $C_2 = 0$. Next observe that C will be a 1 in the case that the addition of P and Q gives a carry of 1 or in the case that the addition of S_1 (the right-most digit of $P + Q$) and R gives a carry of 1. In other words, $C = 1$ if, and only if, $C_1 = 1$ or $C_2 = 1$. It follows that the circuit shown in Figure 2.5.2 will compute the sum of three binary digits.

FULL-ADDER

Circuit



Input/Output Table

P	*Q*	*R*	*C*	*S*
1	1	1	1	1
1	1	0	1	0
1	0	1	1	0
1	0	0	0	1
0	1	1	1	0
0	1	0	0	1
0	0	1	0	1
0	0	0	0	0

FIGURE 2.5.2 Circuit to Add $P + Q + R$, Where P, Q, and R Are Binary Digits

Two full-adders and one half-adder can be used together to build a circuit that will add two three-digit binary numbers PQR and STU to obtain the sum $WXYZ$. This is illustrated in Figure 2.5.3. Such a circuit is called a **parallel adder**. Parallel adders can be constructed to add binary numbers of any finite length.

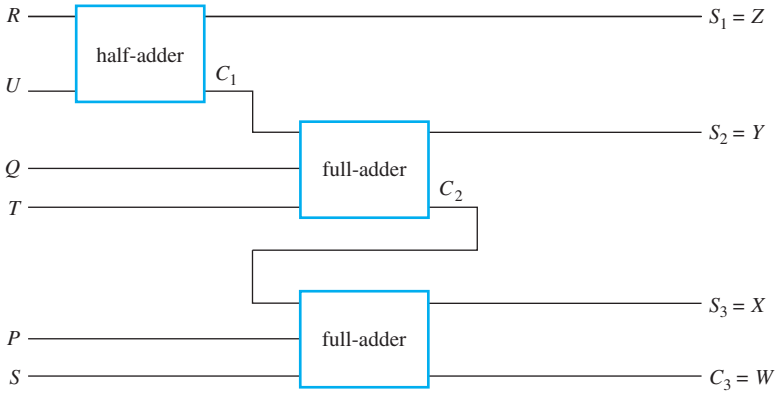


FIGURE 2.5.3 A Parallel Adder to Add PQR and STU to Obtain $WXYZ$

Two's Complements and the Computer Representation of Signed Integers

Typically a fixed number of bits is used to represent integers on a computer. One way to do this is to select a particular bit, normally the left-most, to indicate the sign of the integer, and to use the remaining bits for its absolute value in binary notation. The problem with this approach is that the procedures for adding the resulting numbers are somewhat complicated and the representation of 0 is not unique. A more common approach is to use "two's complements," which makes it possible to add integers quite easily and results in a unique representation for 0. Bit lengths of 64 and (sometimes) 32 are most often used in practice, but, for simplicity and because the principles are the same for all bit lengths, this discussion will focus on a bit length of 8.

We will show how to use eight bits to represent the 256 integers from -128 through 127 and how to perform additions and subtractions within this system of numbers. When the more realistic 32-bit two's complements system is used, more than 4 billion integers can be represented.

Definition

The 8-bit two's complement for an integer a between -128 and 127 is the 8-bit binary representation for $\begin{cases} a & \text{if } a \geq 0 \\ 2^8 - |a| & \text{if } a < 0. \end{cases}$

Thus the 8-bit representation for a nonnegative integer is the same as its 8-bit binary representation. As a concrete example for the negative integer -46, observe that

$$(2^8 - |-46|)_{10} = (256 - 46)_{10} = 210_{10} = (128 + 64 + 16 + 2)_{10} = 11010010_2,$$

and so the 8-bit two's complement for -46 is 11010010.

For negative integers, however, there is a more convenient way to compute two's complements, which involves less arithmetic than applying the definition directly.

The 8-Bit Two's Complement for a Negative Integer

The 8-bit two's complement for a negative integer a that is at least -128 can be obtained as follows:

- Write the 8-bit binary representation for $|a|$.
- Switch all the 1's to 0's and all the 0's to 1's. (This is called flipping, or complementing, the bits.)
- Add 1 in binary notation.

Example 2.5.6 **Finding a Two's Complement**

Use the method described above to find the 8-bit two's complement for -46.

Solution Write the 8-bit binary representation for $|-46|$ $(=46)$, switch all the 1's to 0's and all the 0's to 1's, and then add 1.

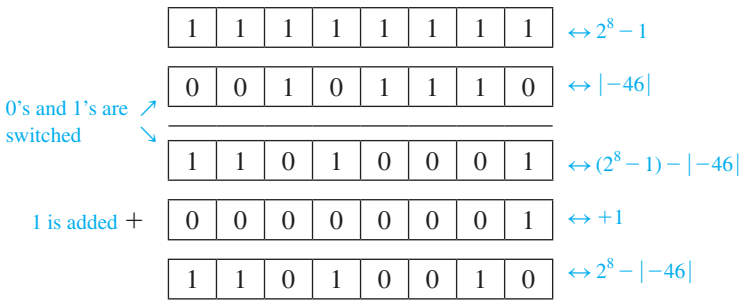
$$|-46|_{10} = 46_{10} = (32+8+4+2)_{10} = 00101110_2 \xrightarrow{\text{flip the bits}} 11010001 \xrightarrow{\text{add 1}} 11010010.$$

Note that this is the same result as was obtained directly from the definition. ■

The fact that the method for finding 8-bit two's complements works in general depends on the following facts:

1. The binary representation of $2^8 - 1$ is 11111111_2.
2. Subtracting an 8-bit binary number a from 11111111_2 switches all the 1's to 0's and all the 0's to 1's.
3. $2^8 - |a| = [(2^8 - 1) - |a|] + 1$ for any number a.

Here is how the facts are used when $a = -46$:



Because 127 is the largest integer represented in the 8-bit two's complement system and because $127_{10} = 01111111_2$, all the 8-bit two's complements for nonnegative integers have a leading bit of 0. Moreover, because the bits are switched, the leading bit for all the negative integers is 1. Table 2.5.2 illustrates the 8-bit two's complement representations for the integers from -128 through 127.

TABLE 2.5.2

Integer	8-Bit Two's Complement	Decimal Form of Two's Complement for Negative Integers
127	01111111	
126	01111110	
⋮	⋮	
2	00000010	
1	00000001	
0	00000000	
−1	11111111	$2^8 - 1$
−2	11111110	$2^8 - 2$
−3	11111101	$2^8 - 3$
⋮	⋮	⋮
−127	10000001	$2^8 - 127$
−128	10000000	$2^8 - 128$

Observe that if the two's complement procedure is used on 11010010, which is the two's complement for −46, the result is

$$11010010 \xrightarrow{\text{flip the bits}} 00101101 \xrightarrow{\text{add 1}} 00101110,$$

which is the two's complement for 46. In general, if the two's complement procedure is applied to a positive or negative integer in two's complement form, the result is the negative (or opposite) of that integer. The only exception is the number −128. (See exercise 37a.)

To find the decimal representation of the negative integer with a given 8-bit two's complement:

- Apply the two's complement procedure to the given two's complement.
- Write the decimal equivalent of the result.

Example 2.5.7 **Finding a Number with a Given Two's Complement**

What is the decimal representation for the integer with two's complement 10101001?

Solution Since the left-most digit is 1, the integer is negative. Applying the two's complement procedure gives the following result:

$$10101001 \xrightarrow{\text{flip the bits}} 01010110 \xrightarrow{\text{add 1}} 01010111_2$$
$$= (64 + 16 + 4 + 2 + 1)_{10} = 87_{10} = |-87|_{10}.$$

So the answer is −87. You can check its correctness by deriving the two's complement of −87 directly from the definition:

$$(2^8 - |-87|)_{10} = (256 - 87)_{10} = 169_{10} = (128 + 32 + 8 + 1)_{10} = 10101001_2. \quad \blacksquare$$

Addition and Subtraction with Integers in Two's Complement Form

The main advantage of a two's complement representation for integers is that the same computer circuits used to add nonnegative integers in binary notation can be used for both additions and subtractions of integers in a two's complement system of numeration. First note that because of the algebraic identity

$$a - b = a + (-b) \text{ for all real numbers,}$$

any subtraction problem can be changed into an addition one. For example, suppose you want to compute $78 - 46$. This equals $78 + (-46)$, which should give an answer of 32. To see what happens when you add the numbers in their two's complement forms, observe that the 8-bit two's complement for 78 is the same as the ordinary binary representation for 78, which is 01001110 because $78 = 64 + 8 + 4 + 2$, and, as previously shown, the 8-bit two's complement for -46 is 11010010. Adding the numbers using binary addition gives the following:

	0	1	0	0	1	1	1	0	$\leftrightarrow 78$
+	1	1	0	1	0	0	1	0	$\leftrightarrow -46$
1	0	0	1	0	0	0	0	0	$\leftrightarrow 32?$

The result has a carry bit of 1 in the ninth, or 2^8th, position, but if you discard it, you obtain 00100000, which *is* the correct answer in 8-bit two's complement form because, since $32 = 2^8$,

$$32_{10} = 00100000_2.$$

In general, if you add numbers in 8-bit two's complement form and get a carry bit of 1 in the ninth, or 2^8th position, you should discard it. Using this procedure is equivalent to reducing the sum of the numbers "modulo 2^8," and it gives results that are correct in ordinary decimal arithmetic as long as the sum of the two numbers is within the fixed-bit-length system of integer representations you are using, in this case those between -128 and 127. The fact that this method produces correct results follows from general properties of modular arithmetic, which is discussed at length in Section 8.4.

General Procedure for Using 8-Bit Two's Complements to Add Two Integers

To add two integers in the range -128 through 127 whose sum is also in the range -128 through 127:

- Convert both integers to their 8-bit two's complement representations.
- Add the resulting integers using ordinary binary addition, discarding any carry bit of 1 that may occur in the 2^8th position.
- Convert the result back to decimal form.

When integers are restricted to the range -128 through 127, you can easily imagine adding two integers and obtaining a sum outside the range. For instance,

$(-87)+(-46) = -133$, which is less than -128 and, therefore, requires more than eight bits for its representation. Because this result is outside the 8-bit fixed-length register system imposed by the architecture of the computer, it is often labeled "overflow error." In the more realistic environment where integers are represented using 64 bits, they can range from less than -10^{19} to more than 10^{19}. So a vast number of integer calculations can be made without producing overflow error. And even if a 32-bit fixed integer length is used, nearly 4 billion integers are represented within the system.

Detecting overflow error turns out to be quite simple. The 8-bit two's complement sum of two integers will be outside the range from -128 through 127 if, and only if, the integers are both positive and the sum computed using 8-bit two's complements is negative, or if the integers are both negative and the sum computed using 8-bit two's complement is positive. To see a concrete example for how this works, consider trying to add (-87) and (-46). Here is what you obtain:

	1	0	1	0	1	0	0	1	$\leftrightarrow -87$
+	1	1	0	1	0	0	1	0	$\leftrightarrow -46$
1	0	1	1	1	1	0	1	1	

When you discard the 1 in the 2^8th position, you find that the leading digit of the result is 0, which would mean that the number with the two's complement representation for the sum of two negative numbers would be positive. So the computer signals an overflow error.*

Hexadecimal Notation

It should now be obvious that numbers written in binary notation take up much more space than numbers written in decimal notation. Yet many aspects of computer operation can best be analyzed using binary numbers. **Hexadecimal notation** is even more compact than decimal notation, and it is much easier to convert back and forth between hexadecimal and binary notation than it is between binary and decimal notation. The word *hexadecimal* comes from the Greek root *hex-*, meaning "six," and the Latin root *deci-*, meaning "ten." Hence *hexadecimal* refers to "sixteen," and hexadecimal notation is also called **base 16 notation**. Hexadecimal notation is based on the fact that any integer can be uniquely expressed as a sum of numbers of the form

$$d \cdot 16^n,$$

where each n is a nonnegative integer and each d is one of the integers from 0 to 15. In order to avoid ambiguity, each hexadecimal digit must be represented by a single symbol. The integers 10 through 15 are represented by the symbols A, B, C, D, E, and F. The 16 hexadecimal digits are shown in Table 2.5.3, together with their decimal equivalents and, for future reference, their 4-bit binary equivalents.

*If the carry bit had not been discarded and if the resulting 9 bits could be processed using a "9-bit two's complement conversion procedure," the result of 101111011 would convert to -133, which is the correct answer. However, the computer signals an error because -133 is not representable within its 8-bit two's complement system.

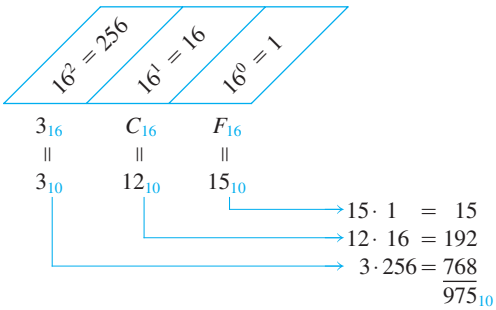
TABLE 2.5.3

Decimal	Hexadecimal	4-Bit Binary Equivalent
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Example 2.5.8 **Converting from Hexadecimal to Decimal Notation**

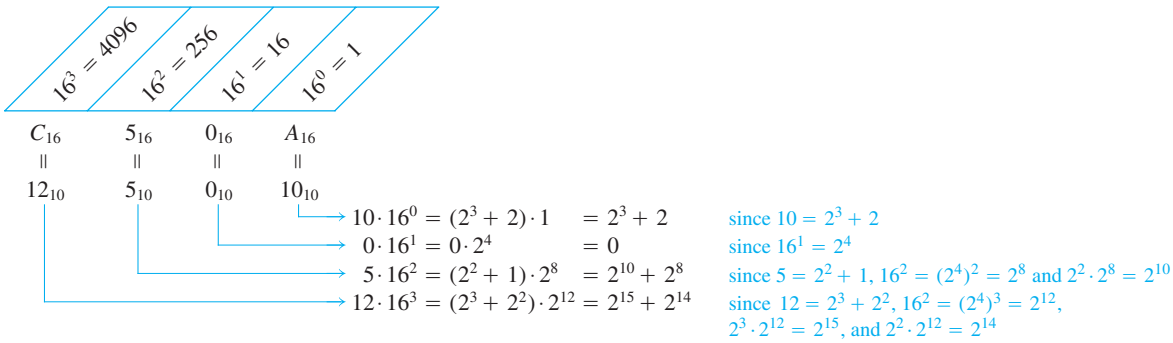
Convert $3CF_{16}$ to decimal notation.

Solution A schema similar to the one introduced in Example 2.5.2 can be used here.



So $3CF_{16} = 975_{10}$. ■

Now consider how to convert from hexadecimal to binary notation. In the example below the numbers are rewritten using powers of 2, and the laws of exponents are applied. The result suggests a general procedure.



But

$$(2^{15} + 2^{14}) + (2^{10} + 2^8) + 0 + (2^3 + 2)$$
$$= 1100\,0000\,0000\,0000_2 + 0101\,0000\,0000_2 \quad \text{by the rules for writing}$$
$$+ 0000\,0000_2 + 1010_2 \quad \text{binary numbers.}$$

So

$$C50A_{16} = \underbrace{1100}_{C_{16}}\ \underbrace{0101}_{5_{16}}\ \underbrace{0000}_{0_{16}}\ \underbrace{1010_2}_{A_{16}}$$

by the rules for adding binary numbers.

The procedure illustrated in this example can be generalized. In fact, the following sequence of steps will always give the correct answer.

To convert an integer from hexadecimal to binary notation:

- Write each hexadecimal digit of the integer in 4-bit binary notation.
- Juxtapose the results.

Example 2.5.9 **Converting from Hexadecimal to Binary Notation**

Convert $B09F_{16}$ to binary notation.

Solution $B_{16} = 11_{10} = 1011_2$, $0_{16} = 0_{10} = 0000_2$, $9_{16} = 9_{10} = 1001_2$, and $F_{16} = 15_{10} = 1111_2$. Consequently,

B	0	9	F
↕	↕	↕	↕
1011	0000	1001	1111

and the answer is 1011000010011111_2. ■

To convert integers written in binary notation into hexadecimal notation, reverse the steps of the previous procedure. Note that the commonly used computer representation for integers uses 32 bits. When these numbers are written in hexadecimal notation only eight characters are needed.

To convert an integer from binary to hexadecimal notation:

- Group the digits of the binary number into sets of four, starting from the right and adding leading zeros as needed.
- Convert the binary numbers in each set of four into hexadecimal digits. Juxtapose those hexadecimal digits.

Example 2.5.10 **Converting from Binary to Hexadecimal Notation**

Convert 100110110101001_2 to hexadecimal notation.

Solution First group the binary digits in sets of four, working from right to left and adding leading 0's if necessary.

0100 1101 1010 1001.

Convert each group of four binary digits into a hexadecimal digit.

0100	1101	1010	1001
↕	↕	↕	↕
4	D	A	9

Then juxtapose the hexadecimal digits.

$$4DA9_{16}$$ ■

Example 2.5.11 **Reading a Memory Dump**

The smallest addressable memory unit on most computers is one byte, or eight bits. In some debugging operations a dump is made of memory contents; that is, the contents of each memory location are displayed or printed out in order. To save space and make the output easier on the eye, the hexadecimal versions of the memory contents are given, rather than the binary versions. Suppose, for example, that a segment of the memory dump looks like

A3 BB 59 2E.

What is the actual content of the four memory locations?

Solution

$$A3_{16} = 10100011_2$$
$$BB_{16} = 10111011_2$$
$$59_{16} = 01011001_2$$
$$2E_{16} = 00101110_2$$ ■

TEST YOURSELF

1. To represent a nonnegative integer in binary notation means to write it as a sum of products of the form _____, where _____.
2. To add integers in binary notation, you use the facts that $1_2 + 1_2 =$ _____ and $1_2 + 1_2 + 1_2 =$ _____.
3. To subtract integers in binary notation, you use the facts that $10_2 - 1_2 =$ _____ and $11_2 - 1_2 =$ _____.
4. A half-adder is a digital logic circuit that _____, and a full-adder is a digital logic circuit that _____.
5. If a is an integer with $-128 \le a \le 127$, the 8-bit two's complement of a is _____ if $a \ge 0$ and is _____ if $a < 0$.
6. To find the 8-bit two's complement of a negative integer a that is at least -128, you _____, _____, and _____.
7. To add two integers in the range -128 through 127 whose sum is also in the range -128 through 127, you _____, _____, _____, and _____.
8. To represent a nonnegative integer in hexadecimal notation means to write it as a sum of products of the form _____, where _____.
9. To convert a nonnegative integer from hexadecimal to binary notation, you _____ and _____.

EXERCISE SET 2.5

Represent the decimal integers in 1–6 in binary notation.

1. 19
2. 55
3. 287
4. 458
5. 1609
6. 1424

Represent the integers in 7–12 in decimal notation.

7. 1110_2
8. 10111_2
9. 110110_2
10. 1100101_2
11. 1000111_2
12. 1011011_2

Perform the arithmetic in 13–20 using binary notation.

13. $1011_2 + 101_2$

14. $1001_2 + 1011_2$

15. $101101_2 + 11101_2$

16. $110111011_2 + 1001011010_2$

17. $10100_2 - 1101_2$

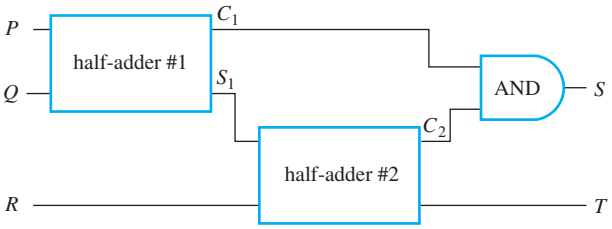
18. $11010_2 - 1101_2$

19. $101101_2 - 10011_2$

20. $1010100_2 - 10111_2$

21. Give the output signals S and T for the circuit shown below if the input signals P, Q, and R are as specified. Note that this is *not* the circuit for a full-adder.

a. $P = 1, Q = 1, R = 1$
b. $P = 0, Q = 1, R = 0$
c. $P = 1, Q = 0, R = 1$



22. Add $11111111_2 + 1_2$ and convert the result to decimal notation, to verify that $11111111_2 = (2^8 - 1)_{10}$.

Find the 8-bit two's complements for the integers in 23–26.

23. -23 **24.** -67 **25.** -4 **26.** -115

Find the decimal representations for the integers with the 8-bit two's complements given in 27–30.

27. 11010011 **28.** 10011001

29. 11110010 **30.** 10111010

Use 8-bit two's complements to compute the sums in 31–36.

31. $57 + (-118)$ **32.** $62 + (-18)$

33. $(-6) + (-73)$ **34.** $89 + (-55)$

35. $(-15) + (-46)$ **36.** $123 + (-94)$

37. a. Show that when you apply the 8-bit two's complement procedure to the 8-bit two's complement for -128, you get the 8-bit two's complement for -128.

***b.** Show that if a, b, and $a + b$ are integers in the range 1 through 128, then

$$(2^8 - a) + (2^8 - b) = (2^8 - (a + b)) + 2^8 \geq 2^8 + 2^7.$$

Explain why it follows that if integers a, b, and $a + b$ are all in the range 1 through 128, then the 8-bit two's complement of $(-a) + (-b)$ is a negative number.

Convert the integers in 38–40 from hexadecimal to decimal notation.

38. $A2BC_{16}$ **39.** $E0D_{16}$ **40.** $39EB_{16}$

Convert the integers in 41–43 from hexadecimal to binary notation.

41. $1C0ABE_{16}$ **42.** $B53DF8_{16}$ **43.** $4ADF83_{16}$

Convert the integers in 44–46 from binary to hexadecimal notation.

44. 00101110_2 **45.** 1011011111000101_2

46. 11001001011100_2

47. Octal Notation: In addition to binary and hexadecimal, computer scientists also use *octal notation* (base 8) to represent numbers. Octal notation is based on the fact that any integer can be uniquely represented as a sum of numbers of the form $d \cdot 8^n$, where each n is a nonnegative integer and each d is one of the integers from 0 to 7. Thus, for example, $5073_8 = 5 \cdot 8^3 + 0 \cdot 8^2 + 7 \cdot 8^1 + 3 \cdot 8^0 = 2619_{10}$.

a. Convert 61502_8 to decimal notation.
b. Convert 20763_8 to decimal notation.
c. Describe methods for converting integers from octal to binary notation and the reverse that are similar to the methods used in Examples 2.5.9 and 2.5.10 for converting back and forth from hexadecimal to binary notation. Give examples showing that these methods result in correct answers.

ANSWERS FOR TEST YOURSELF

1. $d \cdot 2^n$; $d = 0$ or $d = 1$, and n is a nonnegative integer **2.** 10_2; 11_2 **3.** 1_2; 10_2 **4.** outputs the sum of any two binary digits; outputs the sum of any three binary digits **5.** the 8-bit binary representation of a; the 8-bit binary representation of $2^8 - a$ **6.** write the 8-bit binary representation of a; flip the bits; add 1 in binary notation **7.** convert both integers to their 8-bit two's complements; add the results using binary notation; truncate any leading 1; convert back to decimal form **8.** $d \cdot 16^n$; $d = 0, 1, 2, \ldots 9, A, B, C, D, E, F$, and n is a nonnegative integer **9.** write each hexadecimal digit in 4-bit binary notation; juxtapose the results

CHAPTER 3 THE LOGIC OF QUANTIFIED STATEMENTS

In Chapter 2 we discussed the logical analysis of compound statements—those made of simple statements joined by the connectives $\sim$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$. Such analysis casts light on many aspects of human reasoning, but it cannot be used to determine validity in the majority of everyday and mathematical situations. For example, the argument

All men are mortal.
Socrates is a man.
$\therefore$ Socrates is mortal.

is intuitively perceived as correct. Yet its validity cannot be derived using the methods outlined in Section 2.3. To determine validity in examples like this, it is necessary to separate the statements into parts in much the same way that you separate declarative sentences into subjects and predicates. And you must analyze and understand the special role played by words that denote quantities such as "all" or "some." The symbolic analysis of predicates and quantified statements is called the **predicate calculus**. The symbolic analysis of ordinary compound statements (as outlined in Sections 2.1–2.3) is called the **statement calculus** (or the **propositional calculus**).

3.1 Predicates and Quantified Statements I

. . . it was not till within the last few years that it has been realized how fundamental any and some are to the very nature of mathematics. —A. N. Whitehead (1861–1947)

As noted in Section 2.1, the sentence "$x^2 + 2 = 11$" is not a statement because it may be either true or false depending on the value of x. Similarly, the sentence "$x + y > 0$" is not a statement because its truth value depends on the values of the variables x and y.

In grammar, the word *predicate* refers to the part of a sentence that gives information about the subject. In the sentence "James is a student at Bedford College," the word *James* is the subject and the phrase *is a student at Bedford College* is the predicate. The predicate is the part of the sentence from which the subject has been removed.

In logic, predicates can be obtained by removing some or all of the nouns from a statement. For instance, let P stand for "is a student at Bedford College" and let Q stand for "is a student at." Then both P and Q are *predicate symbols*. The sentences "x is a student at Bedford College" and "x is a student at y" are symbolized as $P(x)$ and as $Q(x, y)$, respectively, where x and y are *predicate variables* that take values in appropriate sets. When concrete values are substituted in place of predicate variables, a statement results. For simplicity, we define a *predicate* to be a predicate symbol together with suitable predicate variables. In some other treatments of logic, such objects are referred to as **propositional functions** or **open sentences**.

Definition

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable.

Example 3.1.1 **Finding Truth Values of a Predicate**

Let $P(x)$ be the predicate "$x^2 > x$" with domain the set $\mathbf{R}$ of all real numbers. Write $P(2)$, $P\left(\frac{1}{2}\right)$, and $P\left(-\frac{1}{2}\right)$, and indicate which of these statements are true and which are false.

Solution

$$P(2): \quad 2^2 > 2, \quad \text{or} \quad 4 > 2. \quad \text{True.}$$

$$P\left(\frac{1}{2}\right): \quad \left(\frac{1}{2}\right)^2 > \frac{1}{2}, \quad \text{or} \quad \frac{1}{4} > \frac{1}{2}. \quad \text{False.}$$

$$P\left(-\frac{1}{2}\right): \quad \left(-\frac{1}{2}\right)^2 > -\frac{1}{2} \quad \text{or} \quad \frac{1}{4} > -\frac{1}{2}. \quad \text{True.}$$

■

When an element in the domain of the variable of a one-variable predicate is substituted for the variable, the resulting statement is either true or false. The set of all such elements that make the predicate true is called the *truth set* of the predicate.

Definition

If $P(x)$ is a predicate and x has domain D, the **truth set** of $P(x)$ is the set of all elements of D that make $P(x)$ true when they are substituted for x. The truth set of $P(x)$ is denoted

$$\{x \in D \mid P(x)\}.$$

Note Recall that we read these symbols as "the set of all x in D such that $P(x)$."

Example 3.1.2 **Finding the Truth Set of a Predicate**

Let $Q(n)$ be the predicate "n is a factor of 8." Find the truth set of $Q(n)$ if

a. the domain of n is $\mathbf{Z}^+$, the set of all positive integers

b. the domain of n is $\mathbf{Z}$, the set of all integers.

Solution

a. The truth set is $\{1, 2, 4, 8\}$ because these are exactly the positive integers that divide 8 evenly.

b. The truth set is $\{1, 2, 4, 8, -1, -2, -4, -8\}$ because the negative integers -1, -2, -4, and -8 also divide into 8 without leaving a remainder. ■

The Universal Quantifier: ∀

One sure way to change predicates into statements is to assign specific values to all their variables. For example, if x represents the number 35, the sentence "x is (evenly) divisible by 5" is a true statement since $35 = 5 \cdot 7$. Another way to obtain statements from predicates is to add **quantifiers**. Quantifiers are words that refer to quantities such as "some" or "all"

Fine Art Images/Glow Images

Charles Sanders Peirce (1839–1914)

and tell for how many elements a given predicate is true. The formal concept of quantifier was introduced into symbolic logic in the late nineteenth century by the American philosopher, logician, and engineer Charles Sanders Peirce and, independently, by the German logician Gottlob Frege.

The symbol $\forall$ is called the **universal quantifier**. Depending on the context, it is read as "for every," "for each," "for any," "given any," or "for all." For example, another way to express the sentence "Every human being is mortal" or "All human beings are mortal" is to write

$$\forall \text{ human beings } x,\ x \text{ is mortal},$$

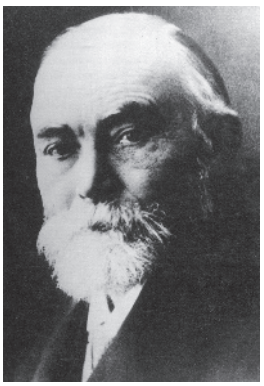
which you would read as "For every human being x, x is mortal." If you let H be the set of all human beings, then you can symbolize the statement more formally by writing

$$\forall x \in H,\ x \text{ is mortal}.$$

Note Think "for every" when you see the symbol $\forall$.

Think of the symbol x as an individual but generic object, with all the properties shared by every human being but with no other properties. Because x is individual, even if you read $\forall$ as "for all," you should use the singular verb and say, "For all x in H, x is mortal" rather than "For all x in H, x are mortal."

In a universally quantified sentence the domain of the predicate variable is generally indicated either between the $\forall$ symbol and the variable name (as in $\forall$ human being x) or immediately following the variable name (as in $\forall x \in H$). In sentences containing a mixture of symbols and words, the $\forall$ symbol can refer to two or more variables. For instance, you could symbolize "For all real numbers x and y, $x + y = y + x$." as "$\forall$ real numbers x and y, $x + y = y + x$."*



Pictorial Press Ltd./Alamy Stock Photo

Gottlob Frege (1848–1925)

Sentences that are quantified universally are defined as statements by giving them the truth values specified in the following definition:

Definition

Let $Q(x)$ be a predicate and D the domain of x. A **universal statement** is a statement of the form "$\forall x \in D$, $Q(x)$." It is defined to be true if, and only if, $Q(x)$ is true for each individual x in D. It is defined to be false if, and only if, $Q(x)$ is false for at least one x in D. A value for x for which $Q(x)$ is false is called a **counterexample** to the universal statement.

Example 3.1.3 **Truth and Falsity of Universal Statements**

a. Let $D = \{1, 2, 3, 4, 5\}$, and consider the statement

$$\forall x \in D,\ x^2 \geq x.$$

Write one way to read this statement out loud, and show that it is true.

b. Consider the statement

$$\forall x \in \mathbf{R},\ x^2 \geq x.$$

Find a counterexample to show that this statement is false.

*More formal versions of symbolic logic would require a separate $\forall$ for each variable: "$\forall x \in \mathbf{R}(\forall y \in \mathbf{R}(x + y = y + x))$."

Solution

a. "For every x in the set D, x^2 is greater than or equal to x." The inequalities below show that "$x^2 \geq x$" is true for each individual x in D.

$$1^2 \geq 1, \qquad 2^2 \geq 2, \qquad 3^2 \geq 3, \qquad 4^2 \geq 4, \qquad 5^2 \geq 5.$$

Hence "$\forall x \in D$, $x^2 \geq x$" is true.

b. *Counterexample:* The statement claims that $x^2 \geq x$ for every real number x. But when $x = \frac{1}{2}$, for example,

$$\left(\frac{1}{2}\right)^2 = \frac{1}{4} \not\geq \frac{1}{2}.$$

Hence "$\forall x \in \mathbf{R}$, $x^2 \geq x$" is false. ■

The technique used to show the truth of the universal statement in Example 3.1.3(a) is called the **method of exhaustion**. It consists of showing the truth of the predicate separately for each individual element of the domain. (The idea is to exhaust the possibilities before you exhaust yourself!) This method can, in theory, be used whenever the domain of the predicate variable is finite. In recent years the prevalence of digital computers has greatly increased the convenience of using the method of exhaustion. Computer expert systems, or knowledge-based systems, use this method to arrive at answers to many of the questions posed to them. Because most mathematical sets are infinite, however, the method of exhaustion can rarely be used to derive general mathematical results.

The Existential Quantifier: ∃

The symbol ∃ denotes "there exists" and is called the **existential quantifier**. For example, the sentence "There is a student in Math 140" can be written as

∃ a person p such that p is a student in Math 140,

Note Think "there exists" when you see the symbol ∃.

or, more formally,

$\exists p \in P$ such that p is a student in Math 140,

where P is the set of all people. The domain of the predicate variable is generally indicated either between the ∃ symbol and the variable name or immediately following the variable name, and the words *such that* are inserted just before the predicate. Some other expressions that can be used in place of *there exists* are *there is a*, *we can find a*, *there is at least one*, *for some*, and *for at least one*. In a sentence such as "∃ integers m and n such that $m + n = m \cdot n$," the ∃ symbol is understood to refer to both m and n.*

Sentences that are quantified existentially are defined as statements by giving them the truth values specified in the following definition.

Definition

Let $Q(x)$ be a predicate and D the domain of x. An **existential statement** is a statement of the form "$\exists x \in D$ such that $Q(x)$." It is defined to be true if, and only if, $Q(x)$ is true for at least one x in D. It is false if, and only if, $Q(x)$ is false for all x in D.

*In more formal versions of symbolic logic, the words *such that* are not written out (although they are understood) and a separate ∃ symbol is used for each variable: "$\exists m \in \mathbf{Z}\ (\exists n \in \mathbf{Z}(m + n = m \cdot n))$."

Example 3.1.4 **Truth and Falsity of Existential Statements**

a. Consider the statement

$$\exists m \in \mathbf{Z}^+ \text{ such that } m^2 = m.$$

Write one way to read this statement out loud, and show that it is true.

b. Let $E = \{5, 6, 7, 8\}$ and consider the statement

$$\exists m \in E \text{ such that } m^2 = m.$$

Show that this statement is false.

Solution

a. "There is at least one positive integer m such that $m^2 = m$." Observe that $1^2 = 1$. Thus "$m^2 = m$" is true for a positive integer m, and so "$\exists m \in \mathbf{Z}^+$ such that $m^2 = m$" is true.

b. Note that $m^2 = m$ is not true for any integers m from 5 through 8:

$$5^2 = 25 \neq 5, \quad 6^2 = 36 \neq 6, \quad 7^2 = 49 \neq 7, \quad 8^2 = 64 \neq 8.$$

Thus "$\exists m \in E$ such that $m^2 = m$" is false. ■

Formal vs. Informal Language

It is important to be able to translate from formal to informal language when trying to make sense of mathematical concepts that are new to you. It is equally important to be able to translate from informal to formal language when thinking out a complicated problem.

Example 3.1.5 **Translating from Formal to Informal Language**

Rewrite the following formal statements in a variety of equivalent but more informal ways. Do not use the symbol $\forall$ or $\exists$.

a. $\forall x \in \mathbf{R}, x^2 \geq 0$.

b. $\forall x \in \mathbf{R}, x^2 \neq -1$.

c. $\exists m \in \mathbf{Z}^+$ such that $m^2 = m$.

Solution

a. Every real number has a nonnegative square.
Or: All real numbers have nonnegative squares.
Or: Any real number has a nonnegative square.
Or: The square of each real number is nonnegative.

b. All real numbers have squares that do not equal -1.
Or: No real numbers have squares equal to -1.
(The words *none are* or *no … are* are equivalent to the words *all are not*.)

c. There is a positive integer whose square is equal to itself.
Or: We can find at least one positive integer equal to its own square.
Or: Some positive integer equals its own square.
Or: Some positive integers equal their own squares. ■

Note In ordinary English, the fourth statement in part (c) may be taken to mean that there are at least two positive integers equal to their own squares. In mathematics, we understand the last two statements in part (c) to mean the same thing.

Another way to restate universal and existential statements informally is to place the quantification at the end of the sentence. For instance, instead of saying "For any real number x, x^2 is nonnegative," you could say "x^2 is nonnegative for any real number x." In such a case the quantifier is said to "trail" the rest of the sentence.

Example 3.1.6 **Trailing Quantifiers**

Rewrite the following statements so that the quantifier trails the rest of the sentence.

a. For any integer n, $2n$ is even.

b. There exists at least one real number x such that $x^2 \leq 0$.

Solution

a. $2n$ is even for any integer n.

b. $x^2 \leq 0$ for some real number x.
Or: $x^2 \leq 0$ for at least one real number x. ■

Example 3.1.7 **Translating from Informal to Formal Language**

Note The following two sentences mean the same thing: "All triangles have three sides" and "Every triangle has three sides."

Rewrite each of the following statements formally. Use quantifiers and variables.

a. All triangles have three sides.

b. No dogs have wings.

c. Some programs are structured.

Solution

a. $\forall$ triangle t, t has three sides.
Or: $\forall t \in T$, t has three sides (where T is the set of all triangles).

b. $\forall$ dog d, d does not have wings.
Or: $\forall d \in D$, d does not have wings (where D is the set of all dogs).

c. $\exists$ a program p such that p is structured.
Or: $\exists p \in P$ such that p is structured (where P is the set of all programs). ■

Universal Conditional Statements

A reasonable argument can be made that the most important form of statement in mathematics is the **universal conditional statement**:

$$\forall x, \text{ if } P(x) \text{ then } Q(x).$$

Familiarity with statements of this form is essential if you are to learn to speak mathematics.

Example 3.1.8 **Writing Universal Conditional Statements Informally**

Rewrite the following statement informally, without quantifiers or variables.

$$\forall x \in \mathbf{R}, \text{ if } x > 2 \text{ then } x^2 > 4.$$

Solution If a real number is greater than 2, then its square is greater than 4.
Or: Whenever a real number is greater than 2, its square is greater than 4.
Or: The square of any real number greater than 2 is greater than 4.
Or: The squares of all real numbers greater than 2 are greater than 4. ■

Example 3.1.9 **Writing Universal Conditional Statements Formally**

Rewrite each of the following statements in the form

$$\forall \_\_\_\_\_, \text{ if } \_\_\_\_\_ \text{ then } \_\_\_\_\_.$$

a. If a real number is an integer, then it is a rational number.

b. All bytes have eight bits.

c. No fire trucks are green.

Solution

a. $\forall$ real number x, if x is an integer, then x is a rational number.
Or: $\forall x \in \mathbf{R}$, if $x \in \mathbf{Z}$ then $x \in \mathbf{Q}$.

b. $\forall x$, if x is a byte, then x has eight bits.

c. $\forall x$, if x is a fire truck, then x is not green.

It is common, as in (b) and (c) above, to omit explicit identification of the domain of predicate variables in universal conditional statements. ■

Careful thought about the meaning of universal conditional statements leads to another level of understanding for why the truth table for an if-then statement must be defined as it is. Consider again the statement

$$\forall \text{ real number } x, \text{ if } x > 2 \text{ then } x^2 > 4.$$

Your experience and intuition tell you that this statement is true. But that means that

$$\text{If } x > 2 \text{ then } x^2 > 4$$

must be true for every single real number x. Consequently, it must be true even for values of x that make its hypothesis "$x > 2$" false. In particular, both statements

$$\text{If } 1 > 2 \text{ then } 1^2 > 4 \quad \text{and} \quad \text{If } -3 > 2 \text{ then } (-3)^2 > 4$$

must be true. In both cases the hypothesis is false, but in the first case the conclusion "$1^2 > 4$" is false, and in the second case the conclusion "$(-3)^2 > 4$" is true. Hence, if an if-then statement has a false hypothesis, we have to interpret it as true regardless of whether its conclusion is true or false.

Note also that the definition of valid argument is a universal conditional statement:

> For every combination of truth values for the component statements,
> if the premises are all true then the conclusion is also true.

Equivalent Forms of Universal and Existential Statements

Observe that the two statements "$\forall$ real number x, if x is an integer then x is rational" and "$\forall$ integer x, x is rational" mean the same thing because the set of integers is a subset of the set of real numbers. Both have informal translations "All integers are rational." In fact, a statement of the form

$$\forall x \in U, \text{ if } P(x) \text{ then } Q(x)$$

can always be rewritten in the form

$$\forall x \in D, Q(x)$$

by narrowing U to be the subset D consisting of all values of the variable x that make $P(x)$ true. Conversely, a statement of the form

$$\forall x \in D, Q(x)$$

can be rewritten as

$$\forall x, \text{ if } x \text{ is in } D \text{ then } Q(x).$$

Example 3.1.10 **Equivalent Forms for Universal Statements**

Rewrite the following statement in the two forms "$\forall x$, if _____ then _____" and "$\forall$ _____ x, _____": All squares are rectangles.

Solution $\forall x$, if x is a square then x is a rectangle.
$\forall$ square x, x is a rectangle. ■

Similarly, a statement of the form "$\exists x$ such that $P(x)$ and $Q(x)$" can be rewritten as "$\exists x \in D$ such that $Q(x)$," where D is the set of all x for which $P(x)$ is true.

Example 3.1.11 **Equivalent Forms for Existential Statements**

A **prime number** is an integer greater than 1 whose only positive integer factors are itself and 1. Consider the statement "There is an integer that is both prime and even." Let Prime(n) be "n is prime" and Even(n) be "n is even." Use the notation Prime(n) and Even(n) to rewrite this statement in the following two forms:

a. $\exists n$ such that _____ $\wedge$ _____.

b. $\exists$ _____ n such that _____.

Solution

a. $\exists n$ such that Prime(n) $\wedge$ Even(n).

b. Two answers: $\exists$ a prime number n such that Even(n).
$\exists$ an even number n such that Prime(n). ■

Bound Variables and Scope

Consider the statement "For every integer x, $x^2 \geq 0$." First note that you don't have to call the variable x. You can use any name for it as long as you do so consistently. For instance, all the following statements have the same meaning:

For every integer x, $x^2 \geq 0$. For every integer n, $n^2 \geq 0$. For every integer s, $s^2 \geq 0$.

In each case the variable simply holds a place for any element in the set of all integers. Each way of writing the statement says that whatever integer you might choose, when you square it the result will be nonnegative. It is important to note, however, that once you finish writing the statement, whatever symbol you chose to use in it can be given an entirely different meaning when used in a different context.

For example, consider the following statements:

(1) For every integer x, $x^2 \geq 0$.

(2) There exists a real number x such that $x^3 = 8$.

Statements (1) and (2) both call the variable x, but the x in Statement (1) serves a different function from the x in Statement (2). We say that the variable x is **bound** by the quantifier that controls it and that its **scope** begins when the quantifier introduces it and ends at the end of the quantified statement.

The way variables are used in mathematics is similar to the way they are used in computer programming. A variable in a computer program also serves as a placeholder in the sense that it creates a location in computer memory (either actual or virtual) into which its values can be placed. In addition the way it can be bound in a program is similar to the

way that a mathematical variable can be bound in a statement. For example, consider the following two examples in Python:

Program 1

```
def f():
  X = "Hi"
  print X
def g():
  X = "Bye"
  print X
f()
g()
```

Program 2

```
def f():
  S = "Hi"
  print S
def g():
  S = "Bye"
  print S
f()
g()
```

The output for both programs is

Hi
Bye

In each case the variable—whether X or S—is **local** to the function where it is defined. It is created each time the function is called and destroyed as soon as the call is complete. The local variable is *bound* by the function that defines it, and its *scope* is restricted to that function. Outside of the function definition the variable name can be used for any other purpose. That is why the functions f and g are allowed to use the same name for the variable in their definitions and why f and g define the same functions in both programs.

Implicit Quantification

Consider the statement

If a number is an integer, then it is a rational number.

As shown earlier, this statement is equivalent to a universal statement. However, it does not contain the telltale word *all* or *every* or *any* or *each*. The only clue to indicate its universal quantification comes from the presence of the indefinite article *a*. This is an example of *implicit* universal quantification.

Existential quantification can also be implicit. For instance, the statement "The number 24 can be written as a sum of two even integers" can be expressed formally as "$\exists$ even integers m and n such that $24 = m + n$."

Mathematical writing contains many examples of implicitly quantified statements. Some occur, as in the first example above, through the presence of the word *a* or *an*. Others occur in cases where the general context of a sentence supplies part of its meaning. For example, in an algebra course in which the letter x is always used to indicate a real number, the predicate

$$\text{If } x > 2 \text{ then } x^2 > 4$$

is interpreted to mean the same as the statement

$$\text{For every real number } x, \text{ if } x > 2 \text{ then } x^2 > 4.$$

Mathematicians often use a double arrow to indicate implicit quantification symbolically. For instance, they might express the above statement as

$$x > 2 \quad \Rightarrow \quad x^2 > 4.$$

Notation

Let $P(x)$ and $Q(x)$ be predicates and suppose the common domain of x is D.

- The notation $\boldsymbol{P(x) \Rightarrow Q(x)}$ means that every element in the truth set of $P(x)$ is in the truth set of $Q(x)$, or, equivalently, $\forall x$, $P(x) \rightarrow Q(x)$.
- The notation $\boldsymbol{P(x) \Leftrightarrow Q(x)}$ means that $P(x)$ and $Q(x)$ have identical truth sets, or, equivalently, $\forall x$, $P(x) \leftrightarrow Q(x)$.

Example 3.1.12 **Using $\Rightarrow$ and $\Leftrightarrow$**

Let

$Q(n)$ be "n is a factor of 8,"

$R(n)$ be "n is a factor of 4,"

$S(n)$ be "$n < 5$ and $n \neq 3$,"

and suppose the domain of n is $\mathbf{Z}^+$, the set of positive integers. Use the $\Rightarrow$ and $\Leftrightarrow$ symbols to indicate true relationships among $Q(n)$, $R(n)$, and $S(n)$.

Solution

1. As noted in Example 3.1.2, the truth set of $Q(n)$ is $\{1, 2, 4, 8\}$ when the domain of n is $\mathbf{Z}^+$. By similar reasoning the truth set of $R(n)$ is $\{1, 2, 4\}$. Thus it is true that every element in the truth set of $R(n)$ is in the truth set of $Q(n)$, or, equivalently, $\forall n$ in $\mathbf{Z}^+$, $R(n) \rightarrow Q(n)$. So $R(n) \Rightarrow Q(n)$, or, equivalently
$$n \text{ is a factor of } 4 \quad \Rightarrow \quad n \text{ is a factor of } 8.$$
2. The truth set of $S(n)$ is $\{1, 2, 4\}$, which is identical to the truth set of $R(n)$, or, equivalently, $\forall n$ in $\mathbf{Z}^+$, $R(n) \leftrightarrow S(n)$. So $R(n) \Leftrightarrow S(n)$, or, equivalently,
$$n \text{ is a factor of } 4 \quad \Leftrightarrow \quad n < 5 \text{ and } n \neq 3.$$
Moreover, since every element in the truth set of $S(n)$ is in the truth set of $Q(n)$, or, equivalently, $\forall n$ in $\mathbf{Z}^+$, $S(n) \rightarrow Q(n)$, then $S(n) \Rightarrow Q(n)$, or, equivalently,
$$n < 5 \text{ and } n \neq 3 \quad \Rightarrow \quad n \text{ is a factor of } 8.$$ ■

Some questions of quantification can be quite subtle. For instance, a mathematics text might contain the following:

a. $(x+1)^2 = x^2 + 2x + 1$. b. Solve $3x - 4 = 5$.

Although neither (a) nor (b) contains explicit quantification, the reader is supposed to understand that the x in (a) is universally quantified, whereas the x in (b) is existentially quantified. When the quantification is made explicit, (a) and (b) become

a. $\forall$ real number x, $(x+1)^2 = x^2 + 2x + 1$.

b. Show (by finding a value) that $\exists$ a real number x such that $3x - 4 = 5$.

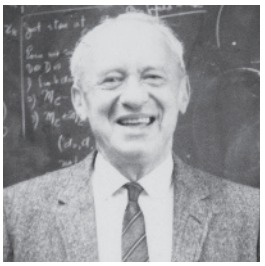
The quantification of a statement—whether universal or existential—crucially determines both how the statement can be applied and what method must be used to establish its truth. Thus it is important to be alert to the presence of hidden quantifiers when you read mathematics so that you will interpret statements in a logically correct way.

Tarski's World

Tarski's World is a computer program developed by information scientists Jon Barwise and John Etchemendy to help teach the principles of logic. It is described in their book

The Language of First-Order Logic, which is accompanied by a CD containing the program Tarski's World, named after the great logician Alfred Tarski.

Example 3.1.13 **Investigating Tarski's World**



Briscoe Center for American History

Alfred Tarski (1902–1983)

The program for Tarski's World provides pictures of blocks of various sizes, shapes, and colors, which are located on a grid. Shown in Figure 3.1.1 is a picture of an arrangement of objects in a two-dimensional Tarski world. The configuration can be described using logical operators and—for the two-dimensional version—notation such as Triangle(x), meaning "x is a triangle," Blue(y), meaning "y is blue," and RightOf(x, y), meaning "x is to the right of y (but possibly in a different row)." Individual objects can be given names such as a, b, or c.

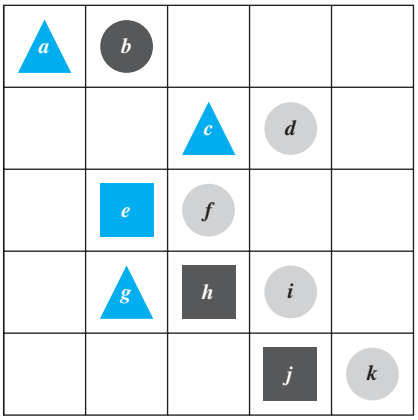


FIGURE 3.1.1

Determine the truth or falsity of each of the following statements. The domain for all variables is the set of objects in the Tarski world shown in Figure 3.1.1.

a. $\forall t$, Triangle(t) $\rightarrow$ Blue(t).

b. $\forall x$, Blue(x) $\rightarrow$ Triangle(x).

c. $\exists y$ such that Square(y) $\wedge$ RightOf(d, y).

d. $\exists z$ such that Square(z) $\wedge$ Gray(z).

Solution

a. This statement is true: Every triangle is blue.

b. This statement is false. As a counterexample, note that e is blue and it is not a triangle.

c. This statement is true because e and h are both square and d is to their right.

d. This statement is false: All the squares are either blue or black. ■

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. If $P(x)$ is a predicate with domain D, the truth set of $P(x)$ is denoted _____. We read these symbols out loud as_____.
2. Some ways to express the symbol $\forall$ in words are _____.
3. Some ways to express the symbol $\exists$ in words are _____.
4. A statement of the form $\forall x \in D$, $Q(x)$ is true if, and only if, $Q(x)$ is _____ for _____.
5. A statement of the form $\exists x \in D$ such that $Q(x)$ is true if, and only if, $Q(x)$ is _____ for _____.

EXERCISE SET 3.1*

1. A menagerie consists of seven brown dogs, two black dogs, six gray cats, ten black cats, five blue birds, six yellow birds, and one black bird. Determine which of the following statements are true and which are false.
   a. There is an animal in the menagerie that is red.
   b. Every animal in the menagerie is a bird or a mammal.
   c. Every animal in the menagerie is brown or gray or black.
   d. There is an animal in the menagerie that is neither a cat nor a dog.
   e. No animal in the menagerie is blue.
   f. There are in the menagerie a dog, a cat, and a bird that all have the same color.

2. Indicate which of the following statements are true and which are false. Justify your answers as best as you can.
   a. Every integer is a real number.
   b. 0 is a positive real number.
   c. For every real number r, $-r$ is a negative real number.
   d. Every real number is an integer.

3. Let $R(m, n)$ be the predicate "If m is a factor of n^2 then m is a factor of n," with domain for both m and n being $\mathbf{Z}$ the set of integers.
   a. Explain why $R(m, n)$ is false if $m = 25$ and $n = 10$.
   b. Give values different from those in part (a) for which $R(m, n)$ is false.
   c. Explain why $R(m, n)$ is true if $m = 5$ and $n = 10$.
   d. Give values different from those in part (c) for which $R(m, n)$ is true.

4. Let $Q(x, y)$ be the predicate "If $x < y$ then $x^2 < y^2$," with domain for both x and y being $\mathbf{R}$ the set of real numbers.
   a. Explain why $Q(x, y)$ is false if $x = -2$ and $y = 1$.
   b. Give values different from those in part (a) for which $Q(x, y)$ is false.
   c. Explain why $Q(x, y)$ is true if $x = 3$ and $y = 8$.
   d. Give values different from those in part (c) for which $Q(x, y)$ is true.

5. Find the truth set of each predicate.
   a. Predicate: $6/d$ is an integer, domain: $\mathbf{Z}$
   b. Predicate: $6/d$ is an integer, domain: $\mathbf{Z}^+$
   c. Predicate: $1 \le x^2 \le 4$, domain: $\mathbf{R}$
   d. Predicate: $1 \le x^2 \le 4$, domain: $\mathbf{Z}$

6. Let $B(x)$ be "$-10 < x < 10$." Find the truth set of $B(x)$ for each of the following domains.
   a. $\mathbf{Z}$ b. $\mathbf{Z}^+$ c. The set of all even integers

7. Let S be the set of all strings of length 3 consisting of a's, b's, and c's. List all the strings in S that satisfy the following conditions:
   1. Every string in S begins with b.
   2. No string in S has more than one c.

8. Let T be the set of all strings of length 3 consisting of 0's and 1's. List all the strings in T that satisfy the following conditions:
   1. For every string s in T, the second character of s is 1 or the first two characters of s are the same.
   2. No string in T has all three characters the same.

Find counterexamples to show that the statements in 9–12 are false.

9. $\forall x \in \mathbf{R}$, $x \ge 1/x$.

10. $\forall a \in \mathbf{Z}$, $(a - 1)/a$ is not an integer.

11. $\forall$ positive integers m and n, $m \cdot n \ge m + n$.

12. $\forall$ real numbers x and y, $\sqrt{x + y} = \sqrt{x} + \sqrt{y}$.

13. Consider the following statement:

    $\forall$ basketball player x, x is tall.

    Which of the following are equivalent ways of expressing this statement?
    a. Every basketball player is tall.
    b. Among all the basketball players, some are tall.
    c. Some of all the tall people are basketball players.
    d. Anyone who is tall is a basketball player.
    e. All people who are basketball players are tall.
    f. Anyone who is a basketball player is a tall person.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

14. Consider the following statement:

$$\exists x \in \mathbf{R} \text{ such that } x^2 = 2.$$

Which of the following are equivalent ways of expressing this statement?

a. The square of each real number is 2.
b. Some real numbers have square 2.
c. The number x has square 2, for some real number x.
d. If x is a real number, then $x^2 = 2$.
e. Some real number has square 2.
f. There is at least one real number whose square is 2.

H **15.** Rewrite the following statements informally in at least two different ways without using variables or quantifiers.

a. $\forall$ rectangle x, x is a quadrilateral.
b. $\exists$ a set A such that A has 16 subsets.

16. Rewrite each of the following statements in the form "$\forall$ _____ x, _____."

a. All dinosaurs are extinct.
b. Every real number is positive, negative, or zero.
c. No irrational numbers are integers.
d. No logicians are lazy.
e. The number 2,147,581,953 is not equal to the square of any integer.
f. The number -1 is not equal to the square of any real number.

17. Rewrite each of the following in the form "$\exists$ _____ x such that _____."

a. Some exercises have answers.
b. Some real numbers are rational.

18. Let D be the set of all students at your school, and let $M(s)$ be "s is a math major," let $C(s)$ be "s is a computer science student," and let $E(s)$ be "s is an engineering student." Express each of the following statements using quantifiers, variables, and the predicates $M(s)$, $C(s)$, and $E(s)$.

a. There is an engineering student who is a math major.
b. Every computer science student is an engineering student.
c. No computer science students are engineering students.
d. Some computer science students are also math majors.
e. Some computer science students are engineering students and some are not.

19. Consider the following statement:

$$\forall \text{ integer } n, \text{ if } n^2 \text{ is even then } n \text{ is even.}$$

Which of the following are equivalent ways of expressing this statement?

a. All integers have even squares and are even.
b. Given any integer whose square is even, that integer is itself even.
c. For all integers, there are some whose square is even.
d. Any integer with an even square is even.
e. If the square of an integer is even, then that integer is even.
f. All even integers have even squares.

H **20.** Rewrite the following statement informally in at least two different ways without using variables or the symbol $\forall$ or the words "for all."

$$\forall \text{ real numbers } x, \text{ if } x \text{ is positive}$$
$$\text{then the square root of } x \text{ is positive.}$$

21. Rewrite the following statements so that the quantifier trails the rest of the sentence.

a. For any graph G, the total degree of G is even.
b. For any isosceles triangle T, the base angles of T are equal.
c. There exists a prime number p such that p is even.
d. There exists a continuous function f such that f is not differentiable.

22. Rewrite each of the following statements in the form "$\forall$ _____ x, if _____ then _____."

a. All Java programs have at least 5 lines.
b. Any valid argument with true premises has a true conclusion.

23. Rewrite each of the following statements in the two forms "$\forall x$, if _____ then _____" and "$\forall x$, _____" (without an if-then).

a. All equilateral triangles are isosceles.
b. Every computer science student needs to take data structures.

24. Rewrite the following statements in the two forms "$\exists$ _____ x such that _____" and "$\exists x$ such that _____ and _____."

a. Some hatters are mad.
b. Some questions are easy.

25. The statement "The square of any rational number is rational" can be rewritten formally as "For all rational numbers x, x^2 is rational" or as "For all x,

if x is rational then x^2 is rational." Rewrite each of the following statements in the two forms "$\forall$ _____ x, _____" and "$\forall x$, if _____, then _____" or in the two forms "$\forall$ _____ x and y, _____" and "$\forall x$ and y, if _____, then _____."

a. The reciprocal of any nonzero fraction is a fraction.
b. The derivative of any polynomial function is a polynomial function.
c. The sum of the angles of any triangle is 180°.
d. The negative of any irrational number is irrational.
e. The sum of any two even integers is even.
f. The product of any two fractions is a fraction.

26. Consider the statement "All integers are rational numbers but some rational numbers are not integers."

a. Write this statement in the form "$\forall x$, if _____ then _____, but $\exists$ _____ x such that _____."
b. Let Ratl(x) be "x is a rational number" and Int(x) be "x is an integer." Write the given statement formally using only the symbols Ratl(x), Int(x), $\forall$, $\exists$, $\wedge$, $\vee$, $\sim$, and $\rightarrow$.

27. Refer to the picture of Tarski's world given in Example 3.1.13. Let Above(x, y) mean that x is above y (but possibly in a different column). Determine the truth or falsity of each of the following statements. Give reasons for your answers.

a. $\forall u$, Circle(u) $\rightarrow$ Gray(u).
b. $\forall u$, Gray(u) $\rightarrow$ Circle(u).
c. $\exists y$ such that Square(y) $\wedge$ Above(y, d).
d. $\exists z$ such that Triangle(z) $\wedge$ Above(f, z).

In 28–30, rewrite each statement without using quantifiers or variables. Indicate which are true and which are false, and justify your answers as best as you can.

28. Let the domain of x be the set D of objects discussed in mathematics courses, and let Real(x) be "x is a real number," Pos(x) be "x is a positive real number," Neg(x) be "x is a negative real number," and Int(x) be "x is an integer."

a. Pos(0)
b. $\forall x$, Real(x) $\wedge$ Neg(x) $\rightarrow$ Pos($-x$)
c. $\forall x$, Int(x) $\rightarrow$ Real(x)
d. $\exists x$ such that Real(x) $\wedge \sim$Int(x)

29. Let the domain of x be the set of geometric figures in the plane, and let Square(x) be "x is a square" and Rect(x) be "x is a rectangle."

a. $\exists x$ such that Rect(x) $\wedge$ Square(x)
b. $\exists x$ such that Rect(x) $\wedge \sim$Square(x)
c. $\forall x$, Square(x) $\rightarrow$ Rect(x)

30. Let the domain of x be **Z**, the set of integers, and let Odd(x) be "x is odd," Prime(x) be "x is prime," and Square(x) be "x is a perfect square." (An integer n is said to be a **perfect square** if, and only if, it equals the square of some integer. For example, 25 is a perfect square because $25 = 5^2$.)

a. $\exists x$ such that Prime(x) $\wedge \sim$Odd(x)
b. $\forall x$, Prime(x) $\rightarrow \sim$Square(x)
c. $\exists x$ such that Odd(x) $\wedge$ Square(x)

H **31.** In any mathematics or computer science text other than this book, find an example of a statement that is universal but is implicitly quantified. Copy the statement as it appears and rewrite it making the quantification explicit. Give a complete citation for your example, including title, author, publisher, year, and page number.

32. Let **R** be the domain of the predicate variable x. Which of the following are true and which are false? Give counter examples for the statements that are false.

a. $x > 2 \Rightarrow x > 1$
b. $x > 2 \Rightarrow x^2 > 4$
c. $x^2 > 4 \Rightarrow x > 2$
d. $x^2 > 4 \Leftrightarrow |x| > 2$

33. Let **R** be the domain of the predicate variables a, b, c, and d. Which of the following are true and which are false? Give counterexamples for the statements that are false.

a. $a > 0$ and $b > 0 \Rightarrow ab > 0$
b. $a < 0$ and $b < 0 \Rightarrow ab < 0$
c. $ab = 0 \Rightarrow a = 0$ or $b = 0$
d. $a < b$ and $c < d \Rightarrow ac < bd$

ANSWERS FOR TEST YOURSELF

1. $\{x \in D | P(x)\}$; the set of all x in D such that $P(x)$ **2.** *Possible answers:* for every, for any, for each, for arbitrary, given any, for all **3.** *Possible answers:* there exists, there exist, there exists at least one, for some, for at least one, we can find a **4.** true; every x in D (*Some alternative answers:* all x in D; each individual x in D) **5.** true; at least one x in D (*Alternative answer:* some x in D)

3.2 Predicates and Quantified Statements II

TOUCHSTONE: *Stand you both forth now: stroke your chins, and swear by your beards that I am a knave.*
CELIA: *By our beards—if we had them—thou art.*
TOUCHSTONE: *By my knavery—if I had it—then I were; but if you swear by that that is not, you are not forsworn.* —William Shakespeare, *As You Like It*

This section continues the discussion of predicates and quantified statements begun in Section 3.1. It contains the rules for negating quantified statements; an exploration of the relation among $\forall$, $\exists$, $\wedge$, and $\vee$; an introduction to the concept of vacuous truth of universal statements; examples of variants of universal conditional statements; and an extension of the meaning of *necessary*, *sufficient*, and *only if* to quantified statements.

Negations of Quantified Statements

Consider the statement "All mathematicians wear glasses." Many people would say that its negation is "No mathematicians wear glasses," but if even one mathematician does not wear glasses, then the sweeping statement that *all* mathematicians wear glasses is false. So a correct negation is "There is at least one mathematician who does not wear glasses."

The general form of the negation of a universal statement follows immediately from the definitions of negation and of the truth values for universal and existential statements.

Theorem 3.2.1 Negation of a Universal Statement

The negation of a statement of the form

$$\forall x \text{ in } D,\ Q(x)$$

is logically equivalent to a statement of the form

$$\exists x \text{ in } D \text{ such that } \sim Q(x).$$

Symbolically,

$$\sim(\forall x \in D,\ Q(x)) \equiv \exists x \in D \text{ such that } \sim Q(x).$$

Thus

> **The negation of a universal statement ("all are") is logically equivalent to an existential statement ("some are not" or "there is at least one that is not").**

Note that when we speak of **logical equivalence for quantified statements**, we mean that the statements always have identical truth values no matter what predicates are substituted for the predicate symbols and no matter what sets are used for the domains of the predicate variables.

Now consider the statement "Some snowflakes are the same." What is its negation? For this statement to be false means that not a single snowflake is the same as any other. In other words, "No snowflakes are the same," or "All snowflakes are different."

The general form for the negation of an existential statement follows immediately from the definitions of negation and of the truth values for existential and universal statements.

Theorem 3.2.2 Negation of an Existential Statement

The negation of a statement of the form

$$\exists x \text{ in } D \text{ such that } Q(x)$$

is logically equivalent to a statement of the form

$$\forall x \text{ in } D, \sim Q(x).$$

Symbolically,

$$\sim(\exists x \in D \text{ such that } Q(x)) \equiv \forall x \in D, \sim Q(x).$$

Thus

The negation of an existential statement ("some are") is logically equivalent to a universal statement ("none are" or "all are not").

Example 3.2.1 **Negating Quantified Statements**

Write formal negations for the following statements:

a. $\forall$ primes p, p is odd.

b. $\exists$ a triangle T such that the sum of the angles of T equals 200°.

Solution

a. By applying the rule for the negation of a $\forall$ statement, you can see that the answer is

$$\exists \text{ a prime } p \text{ such that } p \text{ is not odd.}$$

b. By applying the rule for the negation of a $\exists$ statement, you can see that the answer is

$$\forall \text{ triangles } T, \text{ the sum of the angles of } T \text{ does not equal } 200°.$$ ■

You need to exercise special care to avoid mistakes when writing negations of statements that are given informally. One way to avoid error is to rewrite the statement formally and take the negation using the formal rule.

Example 3.2.2 **More Negations**

Rewrite the following statements formally. Then write formal and informal negations.

a. No politicians are honest.

b. The number 1,357 is not divisible by any integer between 1 and 37.

Solution

a. *Formal version:* $\forall$ politicians x, x is not honest.
Formal negation: $\exists$ a politician x such that x is honest.
Informal negation: Some politicians are honest.

b. This statement has a trailing quantifier. Written formally it becomes:

$$\forall \text{ integer } n \text{ between 1 and 37, 1,357 is not divisible by } n.$$

Note Which is true: the statement in part (b) or its negation? Is 1,357 divisible by some integer between 1 and 37? Or is 1,357 not divisible by any integer between 1 and 37?

Its negation is therefore

$$\exists \text{ an integer } n \text{ between 1 and 37 such that 1,357 is divisible by } n.$$

An informal version of the negation is

The number 1,357 is divisible by some integer between 1 and 37. ■

Another important way to avoid error when taking negations of statements, whether stated formally or informally, is to ask yourself, "What *exactly* would it mean for the given statement to be false? What statement, if true, would be equivalent to saying that the given statement is false?"

Example 3.2.3 **Still More Negations**

Write informal negations for the following statements:

a. All computer programs are finite.

b. Some computer hackers are over 40.

Solution

a. What exactly would it mean for this statement to be false? The statement asserts that all computer programs satisfy a certain property. So for it to be false, there would have to be at least one computer program that does not satisfy the property. Thus the answer is

There is a computer program that is not finite.

Or: Some computer programs are infinite.

b. This statement is equivalent to saying that there is at least one computer hacker with a certain property. So for it to be false, not a single computer hacker can have that property. Thus the negation is

No computer hackers are over 40.

Or: All computer hackers are 40 or under. ■

Caution! Just inserting the word *not* to negate a quantified statement can result in a statement that is ambiguous.

Informal negations of many universal statements can be constructed simply by inserting the word *not* or the words *do not* at an appropriate place. However, the resulting statements may be ambiguous. For example, a possible negation of "All mathematicians wear glasses" is "All mathematicians do not wear glasses." The problem is that this sentence has two meanings. With the proper verbal stress on the word *not*, it could be interpreted as the logical negation. (What! You say that all mathematicians wear glasses? Nonsense! All mathematicians do *not* wear glasses.) On the other hand, stated in a flat tone of voice (try it!), it would mean that all mathematicians are nonwearers of glasses; that is, not a single mathematician wears glasses. This is a much stronger statement than the logical negation: It implies the negation but is not equivalent to it.

Negations of Universal Conditional Statements

Negations of universal conditional statements are of special importance in mathematics. The form of such negations can be derived from facts that have already been established.

By definition of the negation of a *for all* statement,

$$\sim(\forall x, P(x) \to Q(x)) \equiv \exists x \text{ such that } \sim(P(x) \to Q(x)). \qquad 3.2.1$$

But the negation of an if-then statement is logically equivalent to an *and* statement. More precisely,

$$\sim(P(x) \rightarrow Q(x)) \equiv P(x) \wedge \sim Q(x). \qquad 3.2.2$$

Substituting (3.2.2) into (3.2.1) gives

$$\sim(\forall x,\ P(x) \rightarrow Q(x)) \equiv \exists x \text{ such that } (P(x) \wedge \sim Q(x)).$$

Written somewhat less symbolically, this becomes

Negation of a Universal Conditional Statement

$$\sim(\forall x, \text{ if } P(x) \text{ then } Q(x)) \equiv \exists x \text{ such that } P(x) \text{ and } \sim Q(x).$$

Example 3.2.4 **Negating Universal Conditional Statements**

Write a formal negation for statement (a) and an informal negation for statement (b).

a. $\forall$ person p, if p is blond then p has blue eyes.

b. If a computer program has more than 100,000 lines, then it contains a bug.

Solution

a. $\exists$ a person p such that p is blond and p does not have blue eyes.

b. There is at least one computer program that has more than 100,000 lines and does not contain a bug. ■

The Relation among ∀, ∃, ∧, and ∨

The negation of a *for all* statement is a *there exists* statement, and the negation of a *there exists* statement is a *for all* statement. These facts are analogous to De Morgan's laws, which state that the negation of an *and* statement is an *or* statement and that the negation of an *or* statement is an *and* statement. This similarity is not accidental. In a sense, universal statements are generalizations of *and* statements, and existential ments are generalizations of *or* statements.

If $Q(x)$ is a predicate and the domain D of x is the set $\{x_1, x_2, \ldots, x_n\}$, then the statements

$$\forall x \in D,\ Q(x) \quad \text{and} \quad Q(x_1) \wedge Q(x_2) \wedge \cdots \wedge Q(x_n)$$

are logically equivalent. For example, let $Q(x)$ be "$x \cdot x = x$" and suppose $D = \{0, 1\}$. Then

$$\forall x \in D,\ Q(x)$$

can be rewritten as

$$\forall \text{ binary digits } x,\ x \cdot x = x.$$

This is equivalent to

$$0 \cdot 0 = 0 \quad \text{and} \quad 1 \cdot 1 = 1,$$

which can be rewritten in symbols as

$$Q(0) \wedge Q(1).$$

Similarly, if $Q(x)$ is a predicate and $D = \{x_1, x_2, \ldots, x_n\}$, then the statements

$$\exists x \in D \text{ such that } Q(x) \quad \text{and} \quad Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n)$$

are logically equivalent. For example, let $Q(x)$ be "$x + x = x$" and suppose $D = \{0, 1\}$. Then

$$\exists x \in D \text{ such that } Q(x)$$

can be rewritten as

$$\exists \text{ a binary digit } x \text{ such that } x + x = x.$$

This is equivalent to

$$0 + 0 = 0 \quad \text{or} \quad 1 + 1 = 1,$$

which can be rewritten in symbols as

$$Q(0) \vee Q(1).$$

Vacuous Truth of Universal Statements

Suppose a bowl sits on a table and next to the bowl is a pile of five blue and five gray balls, any of which may be placed in the bowl. If three blue balls and one gray ball are placed in the bowl, as shown in Figure 3.2.1(a), the statement "All the balls in the bowl are blue" would be false (since one of the balls in the bowl is gray).

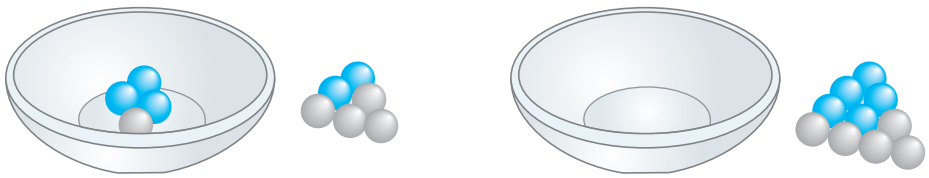
Now suppose that no balls at all are placed in the bowl, as shown in Figure 3.2.1(b). Consider the statement

All the balls in the bowl are blue.

Is this statement true or false? The statement is false if, and only if, its negation is true. And its negation is

There exists a ball in the bowl that is not blue.

But the only way this negation can be true is for there actually to be a nonblue ball in the bowl. And there is not! Hence the negation is false, and so the statement is true "by default."



(a) (b)

FIGURE 3.2.1

Note In ordinary language the words *in general* mean that something is usually, but not always the case. (In general, I take the bus, but today I walked.) In mathematics the words *in general* mean that something is always true.

In general, a statement of the form

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x)$$

is called **vacuously true** or **true by default** if, and only if, $P(x)$ is false for every x in D.

In mathematics, the words *in general* signal that what is to follow is a generalization of some aspect of the example that always holds true.

Variants of Universal Conditional Statements

Recall from Section 2.2 that a conditional statement has a contrapositive, a converse, and an inverse. The definitions of these terms can be extended to universal conditional statements.

Definition

Consider a statement of the form $\forall x \in D$, if $P(x)$ then $Q(x)$.

1. Its **contrapositive** is the statement $\forall x \in D$, if $\sim Q(x)$ then $\sim P(x)$.
2. Its **converse** is the statement $\forall x \in D$, if $Q(x)$ then $P(x)$.
3. Its **inverse** is the statement $\forall x \in D$, if $\sim P(x)$ then $\sim Q(x)$.

Example 3.2.5 **Contrapositive, Converse, and Inverse of a Universal Conditional Statement**

Write a formal and an informal contrapositive, converse, and inverse for the following statement:

If a real number is greater than 2, then its square is greater than 4.

Solution The formal version of this statement is $\forall x \in \mathbf{R}$, if $x > 2$ then $x^2 > 4$.

Contrapositive: $\forall x \in \mathbf{R}$, if $x^2 \leq 4$ then $x \leq 2$.
Or: If the square of a real number is less than or equal to 4, then the number is less than or equal to 2.

Converse: $\forall x \in \mathbf{R}$, if $x^2 > 4$ then $x > 2$.
Or: If the square of a real number is greater than 4, then the number is greater than 2.

Inverse: $\forall x \in \mathbf{R}$, if $x \leq 2$ then $x^2 \leq 4$.
Or: If a real number is less than or equal to 2, then the square of the number is less than or equal to 4.

Note that in solving this example, we have used the equivalence of "$x \not> a$" and "$x \leq a$" for all real numbers x and a. (See page 47.) ■

In Section 2.2 we showed that a conditional statement is logically equivalent to its contrapositive and that it is not logically equivalent to either its converse or its inverse. The following discussion shows that these facts generalize to the case of universal conditional statements and their contrapositives, converses, and inverses.

Let $P(x)$ and $Q(x)$ be any predicates, let D be the domain of x, and consider the statement

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x)$$

and its contrapositive

$$\forall x \in D, \text{ if } \sim Q(x) \text{ then } \sim P(x).$$

Any particular x in D that makes "if $P(x)$ then $Q(x)$" true also makes "if $\sim Q(x)$ then $\sim P(x)$" true (by the logical equivalence between $p \rightarrow q$ and $\sim q \rightarrow \sim p$). It follows that the sentence "If $P(x)$ then $Q(x)$" is true for all x in D if, and only if, the sentence "If $\sim Q(x)$ then $\sim P(x)$" is true for all x in D.

Thus we write the following and say that a universal conditional statement is logically equivalent to its contrapositive:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x) \equiv \forall x \in D, \text{ if } \sim Q(x) \text{ then } \sim P(x)$$

In Example 3.2.5 we noted that the statement

$$\forall x \in \mathbf{R}, \text{ if } x > 2 \text{ then } x^2 > 4$$

has the converse

$$\forall x \in \mathbf{R}, \text{ if } x^2 > 4 \text{ then } x > 2.$$

Observe that the statement is true whereas its converse is false (since, for instance, $(-3)^2 = 9 > 4$ but $-3 \not> 2$). This shows that a universal conditional statement may have a different truth value from its converse. Hence a universal conditional statement is not logically equivalent to its converse. This is written in symbols as follows:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x) \not\equiv \forall x \in D, \text{ if } Q(x) \text{ then } P(x).$$

In exercise 35 at the end of this section, you are asked to provide an example to show that a universal conditional statement is not logically equivalent to its inverse.

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x) \not\equiv \forall x \in D, \text{ if } \sim P(x) \text{ then } \sim Q(x).$$

Necessary and Sufficient Conditions, Only If

The definitions of *necessary*, *sufficient*, and *only if* can also be extended to apply to universal conditional statements.

Definition

- "$\forall x$, $r(x)$ is a **sufficient condition** for $s(x)$" means "$\forall x$, if $r(x)$ then $s(x)$."
- "$\forall x$, $r(x)$ is a **necessary condition** for $s(x)$" means "$\forall x$, if $\sim r(x)$ then $\sim s(x)$" or, equivalently, "$\forall x$, if $s(x)$ then $r(x)$."
- "$\forall x$, $r(x)$ **only if** $s(x)$" means "$\forall x$, if $\sim s(x)$ then $\sim r(x)$" or, equivalently, "$\forall x$, if $r(x)$ then $s(x)$."

Example 3.2.6 **Necessary and Sufficient Conditions**

Rewrite each of the following as a universal conditional statement, quantified either explicitly or implicitly. Do not use the word *necessary* or *sufficient*.

a. Squareness is a sufficient condition for rectangularity.

b. Being at least 35 years old is a necessary condition for being president of the United States.

Solution

a. A formal version of the statement is

$\forall x$, if x is a square, then x is a rectangle.

Or, with implicit universal quantification:

If a figure is a square, then it is a rectangle.

b. Using formal language, you could write the answer as

$\forall$ person x, if x is younger than 35, then x cannot be president of the United States.

Or, by the equivalence between a statement and its contrapositive:

$\forall$ person x, if x is president of the United States, then x is at least 35 years old. ■

Example 3.2.7 **Only If**

Rewrite the following as a universal conditional statement:

A product of two numbers is 0 only if one of the numbers is 0.

Solution Using informal language, you could write the answer as

If it is not the case that one of two numbers is 0,
then the product of the numbers is not 0.

In other words,

If neither of two numbers is 0, then the product of the numbers is not 0.

Or, by the equivalence between a statement and its contrapositive:

If a product of two numbers is 0, then one of the numbers is 0. ■

TEST YOURSELF

1. A negation for "All R have property S" is "There is _____ R that _____."
2. A negation for "Some R have property S" is "_____."
3. A negation for "For every x, if x has property P then x has property Q" is "_____."
4. The converse of "For every x, if x has property P then x has property Q" is "_____."
5. The contrapositive of "For every x, if x has property P then x has property Q" is "_____."
6. The inverse of "For every x, if x has property P then x has property Q" is "_____."

EXERCISE SET 3.2

1. Which of the following is a negation for "All discrete mathematics students are athletic"? More than one answer may be correct.
   a. There is a discrete mathematics student who is nonathletic.
   b. All discrete mathematics students are nonathletic.
   c. There is an athletic person who is not a discrete mathematics student.
   d. No discrete mathematics students are athletic.
   e. Some discrete mathematics students are nonathletic.
   f. No athletic people are discrete mathematics students.
2. Which of the following is a negation for "All dogs are loyal"? More than one answer may be correct.
   a. All dogs are disloyal.
   b. No dogs are loyal.
   c. Some dogs are disloyal.
   d. Some dogs are loyal.
   e. There is a disloyal animal that is not a dog.
   f. There is a dog that is disloyal.
   g. No animals that are not dogs are loyal.
   h. Some animals that are not dogs are loyal.
3. Write a formal negation for each of the following statements.
   a. $\forall$ string s, s has at least one character.
   b. $\forall$ computer c, c has a CPU.
   c. $\exists$ a movie m such that m is over 6 hours long.
   d. $\exists$ a band b such that b has won at least 10 Grammy awards.
4. Write an informal negation for each of the following statements. Be careful to avoid negations that are ambiguous.
   a. All dogs are friendly.
   b. All graphs are connected.
   c. Some suspicions were substantiated.
   d. Some estimates are accurate.
5. Write a negation for each of the following statements.
   a. Every valid argument has a true conclusion.
   b. All real numbers are positive, negative, or zero.

Write a negation for each statement in 6 and 7.

6. a. Sets A and B do not have any points in common.
b. Towns P and Q are not connected by any road on the map.

7. a. This vertex is not connected to any other vertex in the graph.
b. This number is not related to any even number.

8. Consider the statement "There are no simple solutions to life's problems." Write an informal negation for the statement, and then write the statement formally using quantifiers and variables.

Write a negation for each statement in 9 and 10.

9. $\forall$ real number x, if $x > 3$ then $x^2 > 9$.

10. $\forall$ computer program P, if P compiles without error messages, then P is correct.

In each of 11–14 determine whether the proposed negation is correct. If it is not, write a correct negation.

11. *Statement:* The sum of any two irrational numbers is irrational.
Proposed negation: The sum of any two irrational numbers is rational.

12. *Statement:* The product of any irrational number and any rational number is irrational.
Proposed negation: The product of any irrational number and any rational number is rational.

13. *Statement:* For every integer n, if n^2 is even then n is even.
Proposed negation: For every integer n, if n^2 is even then n is not even.

14. *Statement:* For all real numbers x_1 and x_2, if $x_1^2 = x_2^2$ then $x_1 = x_2$.
Proposed negation: For all real numbers x_1 and x_2, if $x_1^2 = x_2^2$ then $x_1 \neq x_2$.

15. Let $D = \{-48, -14, -8, 0, 1, 3, 16, 23, 26, 32, 36\}$. Determine which of the following statements are true and which are false. Provide counterexamples for the statements that are false.
a. $\forall x \in D$, if x is odd then $x > 0$.
b. $\forall x \in D$, if x is less than 0 then x is even.
c. $\forall x \in D$, if x is even then $x \leq 0$.
d. $\forall x \in D$, if the ones digit of x is 2, then the tens digit is 3 or 4.
e. $\forall x \in D$, if the ones digit of x is 6, then the tens digit is 1 or 2.

In 16–23, write a negation for each statement.

16. $\forall$ real number x, if $x^2 \geq 1$ then $x > 0$.

17. $\forall$ integer d, if $6/d$ is an integer then $d = 3$.

18. $\forall x \in \mathbf{R}$, if $x(x+1) > 0$ then $x > 0$ or $x < -1$.

19. $\forall n \in \mathbf{Z}$, if n is prime then n is odd or $n = 2$.

20. $\forall$ integers a, b, and c, if $a - b$ is even and $b - c$ is even, then $a - c$ is even.

21. $\forall$ integer n, if n is divisible by 6, then n is divisible by 2 and n is divisible by 3.

22. If the square of an integer is odd, then the integer is odd.

23. If a function is differentiable then it is continuous.

24. Rewrite the statements in each pair in if-then form and indicate the logical relationship between them.
a. All the children in Tom's family are female.
All the females in Tom's family are children.
b. All the integers that are greater than 5 and end in 1, 3, 7, or 9 are prime.
All the integers that are greater than 5 and are prime end in 1, 3, 7, or 9.

25. Each of the following statements is true. In each case write the converse of the statement, and give a counterexample showing that the converse is false.
a. If n is any prime number that is greater than 2, then $n + 1$ is even.
b. If m is any odd integer, then $2m$ is even.
c. If two circles intersect in exactly two points, then they do not have a common center.

In 26–33, for each statement in the referenced exercise write the contrapositive, converse, and inverse. Indicate as best as you can which of these statements are true and which are false. Give a counterexample for each that is false.

26. Exercise 16 **27.** Exercise 17

28. Exercise 18 **29.** Exercise 19

30. Exercise 20 **31.** Exercise 21

32. Exercise 22 **33.** Exercise 23

34. Write the contrapositive for each of the following statements.
a. If n is prime, then n is not divisible by any prime number from 2 through $\sqrt{n}$. (Assume that n is a fixed integer.)
b. If A and B do not have any elements in common, then they are disjoint. (Assume that A and B are fixed sets.)

35. Give an example to show that a universal conditional statement is not logically equivalent to its inverse.

***36.** If $P(x)$ is a predicate and the domain of x is the set of all real numbers, let R be "$\forall x \in \mathbf{Z}$, $P(x)$," let S be "$\forall x \in \mathbf{Q}$, $P(x)$," and let T be "$\forall x \in \mathbf{R}$, $P(x)$."

a. Find a definition for $P(x)$ (but do not use "$x \in \mathbf{Z}$") so that R is true and both S and T are false.

b. Find a definition for $P(x)$ (but do not use "$x \in \mathbf{Q}$") so that both R and S are true and T is false.

37. Consider the following sequence of digits: 0204. A person claims that all the 1's in the sequence are to the left of all the 0's in the sequence. Is this true? Justify your answer. (*Hint:* Write the claim formally and write a formal negation for it. Is the negation true or false?)

38. True or false? All occurrences of the letter *u* in *Discrete Mathematics* are lowercase. Justify your answer.

Rewrite each statement of 39–44 in if-then form.

39. Earning a grade of C− in this course is a sufficient condition for it to count toward graduation.

40. Being divisible by 8 is a sufficient condition for being divisible by 4.

41. Being on time each day is a necessary condition for keeping this job.

42. Passing a comprehensive exam is a necessary condition for obtaining a master's degree.

43. A number is prime only if it is greater than 1.

44. A polygon is square only if it has four sides.

Use the facts that the negation of a ∀ statement is a ∃ statement and that the negation of an if-then statement is an *and* statement to rewrite each of the statements 45–48 without using the word *necessary* or *sufficient*.

45. Being divisible by 8 is not a necessary condition for being divisible by 4.

46. Having a large income is not a necessary condition for a person to be happy.

47. Having a large income is not a sufficient condition for a person to be happy.

48. Being a polynomial is not a sufficient condition for a function to have a real root.

49. The computer scientists Richard Conway and David Gries once wrote:

> The absence of error messages during translation of a computer program is only a necessary and not a sufficient condition for reasonable [program] correctness.

Rewrite this statement without using the words *necessary* or *sufficient*.

50. A frequent-flyer club brochure states, "You may select among carriers only if they offer the same lowest fare." Assuming that "only if" has its formal, logical meaning, does this statement guarantee that if two carriers offer the same lowest fare, the customer will be free to choose between them? Explain.

ANSWERS FOR TEST YOURSELF

1. some (*Alternative answers:* at least one; an); does not have property S. **2.** No R have property S. **3.** There is an x such that x has property P and x does not have property Q. **4.** For every x, if x has property Q then x has property P. **5.** For every x, if x does not have property Q then x does not have property P. **6.** For every x, if x does not have property P then x does not have property Q.

3.3 Statements with Multiple Quantifiers

It is not enough to have a good mind. The main thing is to use it well. —René Descartes

Imagine you are visiting a factory that manufactures computer microchips. The factory guide tells you,

> "There is a person supervising every detail of the production process."

Note that this statement contains informal versions of both the existential quantifier *there is* and the universal quantifier *every*. Which of the following best describes its meaning?

- There is one single person who supervises all the details of the production process.
- For any particular production detail, there is a person who supervises that detail, but there might be different supervisors for different details.

As it happens, either interpretation could be what the guide meant. (Reread the sentence to be sure you agree!) Taken by itself, his statement is genuinely ambiguous, although other things he may have said (the context for his statement) might have clarified it. In our ordinary lives, we deal with this kind of ambiguity all the time. Usually context helps resolve it, but sometimes we simply misunderstand each other.

In mathematics, formal logic, and computer science, by contrast, it is essential that we all interpret statements in exactly the same way. For instance, the initial stage of software development typically involves careful discussion between a programmer analyst and a client to turn vague descriptions of what the client wants into unambiguous program specifications that client and programmer can mutually agree on.

Because many important technical statements contain both $\exists$ and $\forall$, a convention has developed for interpreting them uniformly. ***When a statement contains more than one kind of quantifier, we imagine the actions suggested by the quantifiers as being performed in the order in which the quantifiers occur.*** For instance, consider a statement of the form

$$\forall x \text{ in set } D, \exists y \text{ in set } E \text{ such that } x \text{ and } y \text{ satisfy property } P(x, y).$$

To show that such a statement is true, you must be able to meet the following challenge:

Note The scope of $\forall x$ extends throughout the statement, whereas the scope of $\exists y$ starts in the middle. That is why the value of y depends on the value of x.

- Imagine that someone is allowed to choose any element whatsoever from the set D, and imagine that the person gives you that element. Call it x.
- The challenge for you is to find an element y in E so that the person's x and your y, taken together, satisfy property $P(x, y)$.

Because you do not have to specify the y until after the other person has specified the x, you are allowed to find a different value of y for each different x you are given.

Example 3.3.1 **Truth of a ∀∃ Statement in a Tarski World**

Consider the Tarski world shown in Figure 3.3.1.

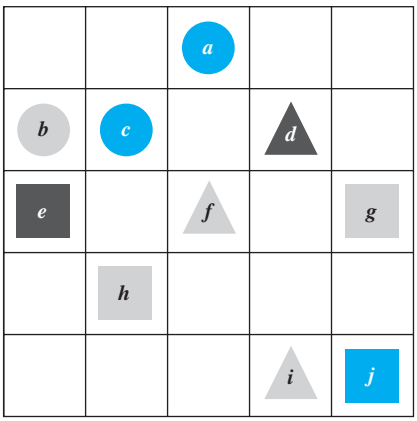


FIGURE 3.3.1

Show that the following statement is true in this world:

For every triangle x, there is a square y such that x and y have the same color.

Solution The statement says that no matter which triangle someone gives you, you will be able to find a square of the same color. There are only three triangles, d, f, and i. The following table shows that for each of these triangles a square of the same color can be found.

Given $x =$	choose $y =$	and check that y is the same color as x.
d	e	yes ✓
f or i	h or g	yes ✓

■

Now consider a statement containing both $\forall$ and $\exists$, where the $\exists$ comes before the $\forall$:

$$\exists x \text{ in set } D \text{ such that } \forall y \text{ in set } E, x \text{ and } y \text{ satisfy property } P(x, y).$$

To show that a statement of this form is true:

You must find one single element (call it x) in D with the following property:

Note The value of x cannot be changed once it is specified because the scope of $\exists x$ extends throughout the entire statement.

- After you have found your x, someone is allowed to choose any element whatsoever from E. The person challenges you by giving you that element. Call it y.
- Your job is to show that your x together with the person's y satisfy property $P(x, y)$.

Your x has to work for *any* y the person might give you; ***you are not allowed to change your x once you have specified it initially.***

Example 3.3.2 **Truth of a ∃∀ Statement in a Tarski World**

Consider again the Tarski world in Figure 3.3.1. Show that the following statement is true: There is a triangle x such that for every circle y, x is to the right of y.

Solution The statement says that you can find a triangle that is to the right of all the circles. Actually, either d or i would work for all of the three circles, a, b, and c, as you can see in the following table.

Choose $x =$	Then: given $y =$	check that x is to the right of y.
d or i	a	yes ✓
	b	yes ✓
	c	yes ✓

■

Here is a summary of the convention for interpreting statements with two different quantifiers:

Interpreting Statements with Two Different Quantifiers

If you want to establish the truth of a statement of the form

$$\forall x \text{ in } D, \exists y \text{ in } E \text{ such that } P(x, y)$$

your challenge is to allow someone else to pick whatever element x in D they wish and then you must find an element y in E that "works" for that particular x.

If you want to establish the truth of a statement of the form

$$\exists x \text{ in } D \text{ such that } \forall y \text{ in } E, P(x, y)$$

your job is to find one particular x in D that will "work" no matter what y in E anyone might choose to challenge you with.

Example 3.3.3 **Interpreting Statements with More Than One Quantifier**

A college cafeteria line has four stations: salads, main courses, desserts, and beverages. The salad station offers a choice of green salad or fruit salad; the main course station offers spaghetti or fish; the dessert station offers pie or cake; and the beverage station offers milk, soda, or coffee. Three students, Uta, Tim, and Yuen, go through the line and make the following choices:

Uta: green salad, spaghetti, pie, milk

Tim: fruit salad, fish, pie, cake, milk, coffee

Yuen: spaghetti, fish, pie, soda

These choices are illustrated in Figure 3.3.2.

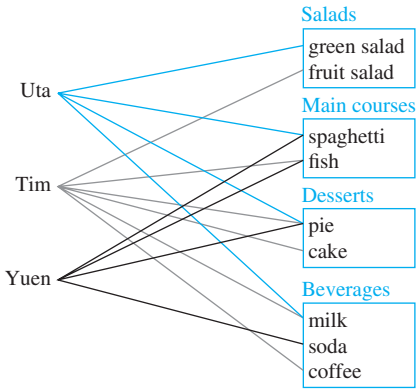


FIGURE 3.3.2

Write each of following statements informally and find its truth value.

a. $\exists$ an item I such that $\forall$ student S, S chose I.

b. $\exists$ a student S such that $\forall$ item I, S chose I.

c. $\exists$ a student S such that $\forall$ station Z, $\exists$ an item I in Z such that S chose I.

d. $\forall$ student S and $\forall$ station Z, $\exists$ an item I in Z such that S chose I.

Solution

a. There is an item that was chosen by every student. This is true; every student chose pie.

b. There is a student who chose every available item. This is false; no student chose all nine items.

c. There is a student who chose at least one item from every station. This is true; both Uta and Tim chose at least one item from every station.

d. Every student chose at least one item from every station. This is false; Yuen did not choose a salad. ■

Translating from Informal to Formal Language

Most problems are stated in informal language, but solving them often requires translating them into more formal terms.

Example 3.3.4 **Translating Statements with Multiple Quantifiers from Informal to Formal Language**

The **reciprocal** of a real number a is a real number b such that $ab = 1$. The following two statements are true. Rewrite them formally using quantifiers and variables.

a. Every nonzero real number has a reciprocal.

b. There is a real number with no reciprocal.

Note The number 0 has no reciprocal.

Solution

a. $\forall$ nonzero real number u, $\exists$ a real number v such that $uv = 1$.

b. $\exists$ a real number c such that $\forall$ real number d, $cd \neq 1$. ■

Example 3.3.5 **There Is a Smallest Positive Integer**

Recall that every integer is a real number and that real numbers are of three types: positive, negative, and zero (zero being neither positive nor negative). Consider the statement "There is a smallest positive integer." Write this statement formally using both symbols $\exists$ and $\forall$.

Solution To say that there is a smallest positive integer means that there is a positive integer m with the property that no matter what positive integer n a person might pick, m will be less than or equal to n:

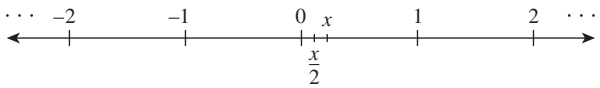
$$\exists \text{ a positive integer } m \text{ such that } \forall \text{ positive integer } n,\ m \leq n.$$

Note that this statement is true because 1 is a positive integer that is less than or equal to every positive integer.

■

Example 3.3.6 **There Is No Smallest Positive Real Number**

Imagine the positive real numbers on the real number line. These numbers correspond to all the points to the right of 0. Observe that no matter how small a real number x is, the number $x/2$ will be both positive and less than x.*



Thus the following statement is true: "There is no smallest positive real number." Write this statement formally using both symbols $\forall$ and $\exists$.

Solution $\forall$ positive real number x, $\exists$ a positive real number y such that $y < x$. ■

Example 3.3.7 **The Definition of Limit of a Sequence**

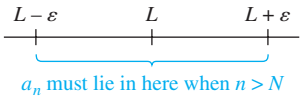
The definition of limit of a sequence, studied in calculus, uses both quantifiers $\forall$ and $\exists$ and also if-then. We say that the limit of the sequence a_n as n goes to infinity equals L and write

$$\lim_{n \to \infty} a_n = L$$

if, and only if, the values of a_n become *arbitrarily* close to L as n gets larger and larger without bound. More precisely, this means that given any positive number ε, we can find

*This can be deduced from the properties of the real numbers given in Appendix A. Because x is positive, $0 < x$. Add x to both sides to obtain $x < 2x$. Then $0 < x < 2x$. Now multiply all parts of the inequality by the positive number 1/2. This does not change the direction of the inequality, so $0 < x/2 < x$.

an integer N such that whenever n is larger than N, the number a_n sits between $L - \varepsilon$ and $L + \varepsilon$ on the number line.



Symbolically:

$$\forall \varepsilon > 0, \exists \text{ an integer } N \text{ such that } \forall \text{ integer } n,$$
$$\text{if } n > N \text{ then } L - \varepsilon < a_n < L + \varepsilon.$$

Considering the logical complexity of this definition, it is no wonder that many students find it hard to understand. ■

Ambiguous Language

The drawing in Figure 3.3.3 is a famous example of visual ambiguity. When you look at it for a while, you will probably see either a silhouette of a young woman wearing a large hat or an elderly woman with a large nose. Whichever image first pops into your mind, try to see how the drawing can be interpreted in the other way. (*Hint:* The mouth of the elderly woman is the necklace on the young woman.)

Chronicle/Alamy Stock Photo

FIGURE 3.3.3

Once most people see one of the images, it is difficult for them to perceive the other. So it is with ambiguous language. Once you interpreted the sentence at the beginning of this section in one way, it may have been hard for you to see that it could be understood in the other way. Perhaps you had difficulty even though the two possible meanings were explained, just as many people have difficulty seeing the second interpretation for the drawing even when they are told what to look for.

Although statements written informally may be open to multiple interpretations, we cannot determine their truth or falsity without interpreting them one way or another. Therefore, we have to use context to try to ascertain their meaning as best we can.

Negations of Statements with More Than One Quantifier

You can use the same rules to negate statements with several quantifiers that you used to negate simpler quantified statements. Recall that

$$\sim(\forall x \text{ in } D,\ P(x)) \equiv \exists x \text{ in } D \text{ such that } \sim P(x).$$

and

$$\sim(\exists x \text{ in } D \text{ such that } P(x)) \equiv \forall x \text{ in } D,\ \sim P(x).$$

Thus

$$\begin{aligned}\sim(\forall x \text{ in } D, \exists y \text{ in } E \text{ such that } P(x, y)) &\equiv \exists x \text{ in } D \text{ such that } \sim(\exists y \text{ in } E \text{ such that } P(x, y)) \\ &\equiv \exists x \text{ in } D \text{ such that } \forall y \text{ in } E,\ \sim P(x, y)\end{aligned}$$

Similarly,

$$\begin{aligned}\sim(\exists x \text{ in } D \text{ such that } \forall y \text{ in } E,\ P(x, y)) &\equiv \forall x \text{ in } D,\ \sim(\forall y \text{ in } E,\ P(x, y)) \\ &\equiv \forall x \text{ in } D, \exists y \text{ in } E \text{ such that } \sim P(x, y)\end{aligned}$$

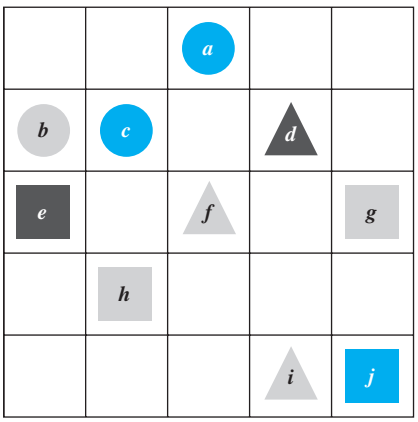
These facts are summarized as follows:

Negations of Statements with Two Different Quantifiers

$$\sim(\forall x \text{ in } D, \exists y \text{ in } E \text{ such that } P(x, y)) \equiv \exists x \text{ in } D \text{ such that } \forall y \text{ in } E,\ \sim P(x, y)$$
$$\sim(\exists x \text{ in } D \text{ such that } \forall y \text{ in } E,\ P(x, y)) \equiv \forall x \text{ in } D, \exists y \text{ in } E \text{ such that } \sim P(x, y)$$

Example 3.3.8 **Negating Statements in a Tarski World**

Refer to the Tarski world of Figure 3.3.1, which is reprinted here for reference.



Write a negation for each of the following statements, and determine which is true, the given statement or its negation.

a. For every square x, there is a circle y such that x and y have the same color.

b. There is a triangle x such that for every square y, x is to the right of y.

Solution

a. *First version of negation:* $\exists$ a square x such that $\sim$($\exists$ a circle y such that x and y have the same color).
Final version of negation: $\exists$ a square x such that $\forall$ circle y, x and y do not have the same color.

The negation is true. Square e is black and no circle in this Tarski world is black, so there is a square that does not have the same color as any circle.

b. *First version of negation:* $\forall$ triangle x, $\sim$($\forall$ square y, x is to the right of y).
Final version of negation: $\forall$ triangle x, $\exists$ a square y such that x is not to the right of y.

The negation is true because no matter what triangle is chosen, it is not to the right of square g or square j, which are the only squares in this Tarski world. ■

Order of Quantifiers

Consider the following two statements:

$$\forall \text{ person } x, \exists \text{ a person } y \text{ such that } x \text{ loves } y.$$
$$\exists \text{ a person } y \text{ such that } \forall \text{ person } x, x \text{ loves } y.$$

Note that except for the order of the quantifiers, these statements are identical. However, the first means that given any person, it is possible to find someone whom that person loves, whereas the second means that there is one amazing individual who is loved by all people. (Reread the statements carefully to verify these interpretations!) The two sentences illustrate an extremely important property about statements with two different quantifiers.

> In a statement containing both $\forall$ and $\exists$, changing the order of the quantifiers can significantly change the meaning of the statement.

Interestingly, however, if one quantifier immediately follows another quantifier *of the same type*, then the order of the quantifiers does not affect the meaning. Consider the commutative property of addition of real numbers, for example:

$$\forall \text{ real number } x \text{ and } \forall \text{ real number } y, x + y = y + x.$$

This means the same as

$$\forall \text{ real number } y \text{ and } \forall \text{ real number } x, x + y = y + x.$$

Thus the property can be expressed a little less formally as

$$\forall \text{ real numbers } x \text{ and } y, x + y = y + x.$$

Example 3.3.9 **Quantifier Order in a Tarski World**

Look again at the Tarski world of Figure 3.3.1. Do the following two statements have the same truth value?

a. For every square x there is a triangle y such that x and y have different colors.

b. There exists a triangle y such that for every square x, x and y have different colors.

Caution! If a statement contains two different quantifiers, reversing their order may change the truth value of the statement to its opposite.

Solution Statement (a) says that if someone gives you one of the squares from the Tarski world, you can find a triangle that has a different color. This is true. If someone gives you square g or h (which are gray), you can use triangle d (which is black); if someone gives you square e (which is black), you can use either triangle f or i (which are gray); and if someone gives you square j (which is blue), you can use triangle d (which is black) or triangle f or i (which are gray).

Statement (b) says that there is one particular triangle in the Tarski world that has a different color from every one of the squares in the world. This is false. Two of the triangles are gray, but they cannot be used to show the truth of the statement because the Tarski world contains gray squares. The only other triangle is black, but it cannot be used either because there is a black square in the Tarski world.

Thus one of the statements is true and the other is false, and so they have opposite truth values. ■

Formal Logical Notation

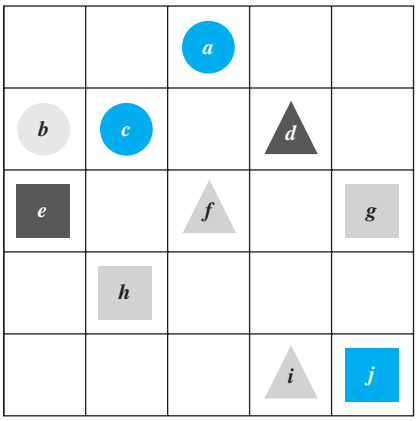
In some areas of computer science, logical statements are expressed in purely symbolic notation. The notation involves using predicates to describe all properties of variables and omitting the words *such that* in existential statements. (When you try to figure out the meaning of a formal statement, however, it is helpful to think the words *such that* to yourself each time they are appropriate.) The formalism also depends on the following facts:

"$\forall x$ in D, $P(x)$" can be written as "$\forall x$ (x in $D \rightarrow P(x)$)," and
"$\exists x$ in D such that $P(x)$" can be written as "$\exists x$ (x in $D \wedge P(x)$)."

We illustrate the use of these facts in Example 3.3.10.

Example 3.3.10 **Formalizing Statements in a Tarski World**

Consider once more the Tarski world of Figure 3.3.1:



Let Triangle(x), Circle(x), and Square(x) mean "x is a triangle," "x is a circle," and "x is a square"; let Blue(x), Gray(x), and Black(x) mean "x is blue," "x is gray," and "x is black"; let RightOf(x, y), Above(x, y), and SameColorAs(x, y) mean "x is to the right of y," "x is above y," and "x has the same color as y"; and use the notation $x = y$ to denote the predicate "x is equal to y." Let the common domain D of all variables be the set of all the objects in the Tarski world. Use formal logical notation to write each of the following statements, and write a formal negation for each statement.

a. For every circle x, x is above f.

b. There is a square x such that x is black.

c. For every circle x, there is a square y such that x and y have the same color.

d. There is a square x such that for every triangle y, x is to the right of y.

Solution

a. *Statement:* $\forall x(\text{Circle}(x) \rightarrow \text{Above}(x, f))$
Negation: $\sim(\forall x\,(\text{Circle}(x) \rightarrow \text{Above}(x, f)))$
$\equiv \exists x \sim(\text{Circle}(x) \rightarrow \text{Above}(x, f))$
by the law for negating a $\forall$ statement
$\equiv \exists x(\text{Circle}(x) \wedge \sim\text{Above}(x, f))$
by the law of negating an if-then statement

b. *Statement:* $\exists x(\text{Square}(x) \wedge \text{Black}(x))$
Negation: $\sim(\exists x(\text{Square}(x) \wedge \text{Black}(x)))$
$\equiv \forall x \sim(\text{Square}(x) \wedge \text{Black}(x))$
by the law for negating a $\exists$ statement
$\equiv \forall x(\sim\text{Square}(x) \vee \sim\text{Black}(x))$
by De Morgan's law

c. *Statement:* $\forall x(\text{Circle}(x) \rightarrow \exists y(\text{Square}(y) \wedge \text{SameColor}(x, y)))$
Negation: $\sim(\forall x(\text{Circle}(x) \rightarrow \exists y(\text{Square}(y) \wedge \text{SameColor}(x, y))))$
$\equiv \exists x \sim(\text{Circle}(x) \rightarrow \exists y(\text{Square}(y) \wedge \text{SameColor}(x, y)))$
by the law for negating a $\forall$ statement
$\equiv \exists x(\text{Circle}(x) \wedge \sim(\exists y(\text{Square}(y) \wedge \text{SameColor}(x, y))))$
by the law for negating an if-then statement
$\equiv \exists x(\text{Circle}(x) \wedge \forall y(\sim(\text{Square}(y) \wedge \text{SameColor}(x, y))))$
by the law for negating a $\exists$ statement
$\equiv \exists x(\text{Circle}(x) \wedge \forall y(\sim\text{Square}(y) \vee \sim\text{SameColor}(x, y)))$
by De Morgan's law

d. *Statement:* $\exists x(\text{Square}(x) \wedge \forall y(\text{Triangle}(y) \rightarrow \text{RightOf}(x, y)))$
Negation: $\sim(\exists x(\text{Square}(x) \wedge \forall y(\text{Triangle}(y) \rightarrow \text{RightOf}(x, y))))$
$\equiv \forall x \sim(\text{Square}(x) \wedge \forall y(\text{Triangle}(x) \rightarrow \text{RightOf}(x, y)))$
by the law for negating a $\exists$ statement
$\equiv \forall x(\sim\text{Square}(x) \vee \sim(\forall y(\text{Triangle}(y) \rightarrow \text{RightOf}(x, y))))$
by De Morgan's law
$\equiv \forall x(\sim\text{Square}(x) \vee \exists y(\sim(\text{Triangle}(y) \rightarrow \text{RightOf}(x, y))))$
by the law for negating a $\forall$ statement
$\equiv \forall x(\sim\text{Square}(x) \vee \exists y(\text{Triangle}(y) \wedge \sim\text{RightOf}(x, y)))$
by the law for negating an if-then statement

■

The disadvantage of the fully formal notation is that because it is complex and somewhat remote from intuitive understanding, when we use it, we may make errors that go unrecognized. The advantage, however, is that operations, such as taking negations, can be made completely mechanical and programmed on a computer. Also, when we become comfortable with formal manipulations, we can use them to check our intuition, and then we can use our intuition to check our formal manipulations. Formal logical notation is used in branches of computer science such as artificial intelligence, program verification, and automata theory and formal languages.

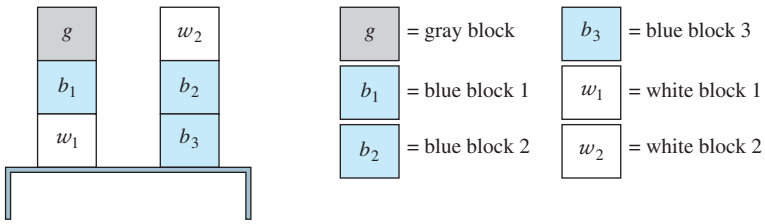
Taken together, the symbols for quantifiers, variables, predicates, and logical connectives make up what is known as the **language of first-order logic**. Even though this language is simpler in many respects than the language we use every day, learning it requires the same kind of practice needed to acquire any foreign language.

Prolog

The programming language Prolog (short for *pro*gramming in *log*ic) was developed in France in the 1970s by A. Colmerauer and P. Roussel to help programmers working in the field of artificial intelligence. A simple Prolog program consists of a set of statements describing some situation together with questions about the situation. Built into the language are search and inference techniques needed to answer the questions by deriving the answers from the given statements. This frees the programmer from the necessity of having to write separate programs to answer each type of question. Example 3.3.11 gives a very simple example of a Prolog program.

Example 3.3.11 **A Prolog Program**

Consider the following picture, which shows colored blocks stacked on a table.



Note Different Prolog implementations follow different conventions as to how to represent constant, variable, and predicate names and forms of questions and answers. The conventions used here are similar to those of Edinburgh Prolog.

The following are statements in Prolog that describe this picture and ask two questions about it.

isabove(g, b_1)	color(g, gray)	color(b_3, blue)
isabove(b_1, w_1)	color(b_1, blue)	color(w_1, white)
isabove(w_2, b_2)	color(b_2, blue)	color(w_2, white)
isabove(b_2, b_3)	isabove(X, Z) if isabove(X, Y) and isabove(Y, Z)	
1. ?color(b_1, blue)	2. ?isabove(X, w_1)	

The statements "isabove(g, b_1)" and "color(g, gray)" are to be interpreted as "g is above b_1" and "g is colored gray." The statement "isabove(X, Z) if isabove(X, Y) and isabove(Y, Z)" is to be interpreted as "For all X, Y, and Z, if X is above Y and Y is above Z, then X is above Z." Statement 1

?color(b_1, blue)

asks whether block b_1 is colored blue. Prolog answers this by writing

Yes.

Statement 2

?isabove(X, w_1)

asks for which blocks X the predicate "X is above w_1" is true. Prolog answers by giving a list of all such blocks. In this case, the answer is

$$X = b_1, X = g.$$

Note that Prolog can find the solution $X = b_1$ by merely searching the original set of given facts. However, Prolog must *infer* the solution $X = g$ from the following statements:

isabove(g, b_1),
isabove(b_1, w_1),
isabove(X, Z) if isabove(X, Y) and isabove(Y, Z).

Write the answers Prolog would give if the following questions were added to the program above.

a. ?isabove(b_2, w_1) b. ?color(w_1, X) c. ?color(X, blue)

Solution

a. The question means "Is b_2 above w_1?"; so the answer is "No."

b. The question means "For what colors X is the predicate 'w_1 is colored X ' true?"; so the answer is "X = white."

c. The question means "For what blocks is the predicate 'X is colored blue' true?"; so the answer is "$X = b_1$," "$X = b_2$," and "$X = b_3$." ■

TEST YOURSELF

1. To establish the truth of a statement of the form "$\forall x$ in D, $\exists y$ in E such that $P(x, y)$," you imagine that someone has given you an element x from D but that you have no control over what that element is. Then you need to find _____ with the property that the x the person gave you together with the _____ you subsequently found satisfy _____.

2. To establish the truth of a statement of the form "$\exists x$ in D such that $\forall y$ in E, $P(x, y)$," you need to find _____ so that no matter what _____ a person might subsequently give you, _____ will be true.

3. Consider the statement "$\forall x$, $\exists y$ such that $P(x, y)$, a property involving x and y, is true." A negation for this statement is "_____."

4. Consider the statement "$\exists x$ such that $\forall y$, $P(x, y)$, a property involving x and y, is true." A negation for this statement is "_____."

5. Suppose $P(x, y)$ is some property involving x and y, and suppose the statement "$\forall x$ in D, $\exists y$ in E such that $P(x, y)$" is true. Then the statement "$\exists x$ in D such that $\forall y$ in E, $P(x, y)$"
   a. is true.
   b. is false.
   c. may be true or may be false.

EXERCISE SET 3.3

1. Let C be the set of cities in the world, let N be the set of nations in the world, and let $P(c, n)$ be "c is the capital city of n." Determine the truth values of the following statements.
a. P(Tokyo, Japan) **b.** P(Athens, Egypt)
c. P(Paris, France) **d.** P(Miami, Brazil)

2. Let $G(x, y)$ be "$x^2 > y$." Indicate which of the following statements are true and which are false.
a. $G(2, 3)$ **b.** $G(1, 1)$
c. $G\left(\frac{1}{2}, \frac{1}{2}\right)$ **d.** $G(-2, 2)$

3. The following statement is true: "$\forall$ nonzero number x, $\exists$ a real number y such that $xy = 1$." For each x given below, find a y to make the predicate "$xy = 1$" true.
a. $x = 2$ **b.** $x = -1$ **c.** $x = 3/4$

4. The following statement is true: "$\forall$ real number x, $\exists$ an integer n such that $n > x$."* For each x given below, find an n to make the predicate "$n > x$" true.
a. $x = 15.83$ **b.** $x = 10^8$ **c.** $x = 10^{10^{10}}$

The statements in exercises 5–8 refer to the Tarski world given in Figure 3.3.1. Explain why each is true.

5. For every circle x there is a square y such that x and y have the same color.

6. For every square x there is a circle y such that x and y have different colors and y is above x.

7. There is a triangle x such that for every square y, x is above y.

8. There is a triangle x such that for every circle y, y is above x.

9. Let $D = E = \{-2, -1, 0, 1, 2\}$. Explain why the following statements are true.
a. $\forall x$ in D, $\exists y$ in E such that $x + y = 0$.
b. $\exists x$ in D such that $\forall y$ in E, $x + y = y$.

10. This exercise refers to Example 3.3.3. Determine whether each of the following statements is true or false.
a. $\forall$ student S, $\exists$ a dessert D such that S chose D.
b. $\forall$ student S, $\exists$ a salad T such that S chose T.
c. $\exists$ a dessert D such that $\forall$ student S, S chose D.
d. $\exists$ a beverage B such that $\forall$ student D, D chose B.
e. $\exists$ an item I such that $\forall$ student S, S did not choose I.
f. $\exists$ a station Z such that $\forall$ student S, $\exists$ an item I such that S chose I from Z.

11. Let S be the set of students at your school, let M be the set of movies that have ever been released, and let $V(s, m)$ be "student s has seen movie m." Rewrite each of the following statements without using the symbol $\forall$, the symbol $\exists$, or variables.
a. $\exists s \in S$ such that $V(s,$ Casablanca).
b. $\forall s \in S$, $V(s,$ Star Wars).
c. $\forall s \in S, \exists m \in M$ such that $V(s, m)$.
d. $\exists m \in M$ such that $\forall s \in S$, $V(s, m)$.
e. $\exists s \in S, \exists t \in S$, and $\exists m \in M$ such that $s \neq t$ and $V(s, m) \wedge V(t, m)$.
f. $\exists s \in S$ and $\exists t \in S$ such that $s \neq t$ and $\forall m \in M$, $V(s, m) \rightarrow V(t, m)$.

12. Let $D = E = \{-2, -1, 0, 1, 2\}$. Write negations for each of the following statements and determine which is true, the given statement or its negation.
a. $\forall x$ in D, $\exists y$ in E such that $x + y = 1$.
b. $\exists x$ in D such that $\forall y$ in E, $x + y = -y$.
c. $\forall x$ in D, $\exists y$ in E such that $xy \geq y$.
d. $\exists x$ in D such that $\forall y$ in E, $x \leq y$.

In each of 13–19, (a) rewrite the statement in English without using the symbol $\forall$ or $\exists$ or variables and expressing your answer as simply as possible, and (b) write a negation for the statement.

13. $\forall$ color C, $\exists$ an animal A such that A is colored C.

14. $\exists$ a book b such that $\forall$ person p, p has read b.

15. $\forall$ odd integer n, $\exists$ an integer k such that $n = 2k + 1$.

16. $\exists$ a real number u such that $\forall$ real number v, $uv = v$.

17. $\forall r \in \mathbf{Q}$, $\exists$ integers a and b such that $r = a/b$.

18. $\forall x \in \mathbf{R}$, $\exists$ a real number y such that $x + y = 0$.

19. $\exists x \in \mathbf{R}$ such that for every real number y, $x + y = 0$.

20. Recall that reversing the order of the quantifiers in a statement with two different quantifiers may

*This is called the Archimedean principle because it was first formulated (in geometric terms) by the great Greek mathematician Archimedes of Syracuse, who lived from about 287 to 212 B.C.E.

change the truth value of the statement—but it does not necessarily do so. All the statements in the pairs below refer to the Tarski world of Figure 3.3.1. In each pair, the order of the quantifiers is reversed but everything else is the same. For each pair, determine whether the statements have the same or opposite truth values. Justify your answers.

a. (1) For every square y there is a triangle x such that x and y have different colors.
(2) There is a triangle x such that for every square y, x and y have different colors.

b. (1) For every circle y there is a square x such that x and y have the same color.
(2) There is a square x such that for every circle y, x and y have the same color.

21. For each of the following equations, determine which of the following statements are true:
(1) For every real number x, there exists a real number y such that the equation is true.
(2) There exists a real number x, such that for every real number y, the equation is true.

Note that it is possible for both statements to be true or for both to be false.

a. $2x + y = 7$
b. $y + x = x + y$
c. $x^2 - 2xy + y^2 = 0$
d. $(x - 5)(y - 1) = 0$
e. $x^2 + y^2 = -1$

In 22 and 23, rewrite each statement without using variables or the symbol ∀ or ∃. Indicate whether the statement is true or false.

22. **a.** ∀ real number x, ∃ a real number y such that $x + y = 0$.
b. ∃ a real number y such that ∀ real number x, $x + y = 0$.

23. **a.** ∀ nonzero real number r, ∃ a real number s such that $rs = 1$.
b. ∃ a real number r such that ∀ nonzero real number s, $rs = 1$.

24. Use the laws for negating universal and existential statements to derive the following rules:

a. $\sim(\forall x \in D(\forall y \in E(P(x, y)))) \equiv \exists x \in D(\exists y \in E(\sim P(x, y)))$

b. $\sim(\exists x \in D(\exists y \in E(P(x, y)))) \equiv \forall x \in D(\forall y \in E(\sim P(x, y)))$

Each statement in 25–28 refers to the Tarski world of Figure 3.3.1. For each, (a) determine whether the statement is true or false and justify your answer, and (b) write a negation for the statement (referring, if you wish, to the result in exercise 24).

25. ∀ circle x and ∀ square y, x is above y.

26. ∀ circle x and ∀ triangle y, x is above y.

27. ∃ a circle x and ∃ a square y such that x is above y and x and y have different colors.

28. ∃ a triangle x and ∃ a square y such that x is above y and x and y have the same color.

For each of the statements in 29 and 30, (a) write a new statement by interchanging the symbols ∀ and ∃, and (b) state which is true: the given statement, the version with interchanged quantifiers, neither, or both.

29. $\forall x \in \mathbf{R}, \exists y \in \mathbf{R}$ such that $x < y$.

30. $\exists x \in \mathbf{R}$ such that $\forall y \in \mathbf{R}^-$ (the set of negative real numbers), $x > y$.

31. Consider the statement "Everybody is older than somebody." Rewrite this statement in the form "∀ people x, ∃ _____."

32. Consider the statement "Somebody is older than everybody." Rewrite this statement in the form "∃ a person x such that ∀ _____."

In 33–39, (a) rewrite the statement formally using quantifiers and variables, and (b) write a negation for the statement.

33. Everybody loves somebody.

34. Somebody loves everybody.

35. Everybody trusts somebody.

36. Somebody trusts everybody.

37. Any even integer equals twice some integer.

38. Every action has an equal and opposite reaction.

39. There is a program that gives the correct answer to every question that is posed to it.

40. In informal speech most sentences of the form "There is _____ every _____" are intended to be understood as meaning "∀ _____ ∃ _____," even though the existential quantifier *there is* comes before the universal quantifier *every*. Note that this interpretation applies to the following

well-known sentences. Rewrite them using quantifiers and variables.

a. There is a sucker born every minute.

b. There is a time for every purpose under heaven.

41. Indicate which of the following statements are true and which are false. Justify your answers as best you can.

a. $\forall x \in \mathbf{Z}^+, \exists y \in \mathbf{Z}^+$ such that $x = y + 1$.

b. $\forall x \in \mathbf{Z}, \exists y \in \mathbf{Z}$ such that $x = y + 1$.

c. $\exists x \in \mathbf{R}$ such that $\forall y \in \mathbf{R}$, $x = y + 1$.

d. $\forall x \in \mathbf{R}^+, \exists y \in \mathbf{R}^+$ such that $xy = 1$.

e. $\forall x \in \mathbf{R}, \exists y \in \mathbf{R}$ such that $xy = 1$.

f. $\exists x \in \mathbf{R}$ such that $\forall y \in \mathbf{R}$, $x + y = y$.

g. $\forall x \in \mathbf{R}^+, \exists y \in \mathbf{R}^+$ such that $y < x$.

h. $\exists x \in \mathbf{R}^+$ such that $\forall y \in \mathbf{R}^+$, $x \leq y$.

42. Write the negation of the definition of limit of a sequence given in Example 3.3.7.

43. The following is the definition for $\lim_{x \to a} f(x) = L$:

For every real number $\varepsilon > 0$, there exists a real number $\delta > 0$ such that for every real number x, if $a - \delta < x < a + \delta$ and $x \neq a$ then

$$L - \varepsilon < f(x) < L + \varepsilon.$$

Write what it means for $\lim_{x \to a} f(x) \neq L$. In other words, write the negation of the definition.

44. The notation $\exists!$ stands for the words "there exists a unique." Thus, for instance, "$\exists!$ x such that x is prime and x is even" means that there is one and only one even prime number. Which of the following statements are true and which are false? Explain.

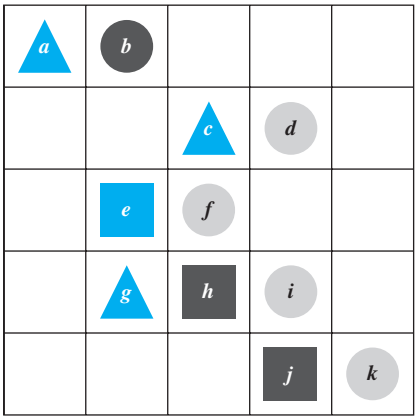
a. $\exists!$ real number x such that $\forall$ real number y, $xy = y$.

b. $\exists!$ integer x such that $1/x$ is an integer.

c. $\forall$ real number x, $\exists!$ real number y such that $x + y = 0$.

***45.** Suppose that $P(x)$ is a predicate and D is the domain of x. Rewrite the statement "$\exists!$ $x \in D$ such that $P(x)$" without using the symbol $\exists!$. (See exercise 44 for the meaning of $\exists!$.)

In 46–54, refer to the Tarski world given in Figure 3.1.1, which is shown again here for reference. The domains of all variables consist of all the objects in the Tarski world. For each statement, (a) indicate whether the statement is true or false and justify your answer, (b) write the given statement using the formal logical notation illustrated in Example 3.3.10, and (c) write a negation for the given statement using the formal logical notation of Example 3.3.10.



46. There is a triangle x such that for every square y, x is above y.

47. There is a triangle x such that for every circle y, x is above y.

48. For every circle x, there is a square y such that y is to the right of x.

49. For every object x, if x is a circle then there is a square y such that y has the same color as x.

50. For every object x, if x is a triangle then there is a square y such that y is below x.

51. There is a square x such that for every triangle y, if y is above x then y has the same color as x.

52. For every circle x and for every triangle y, x is to the right of y.

53. There is a circle x and there is a square y such that x and y have the same color.

54. There is a circle x and there is a triangle y such that x has the same color as y.

Let $P(x)$ and $Q(x)$ be predicates and suppose D is the domain of x. In 55–58, for the statement forms in each pair, determine whether (a) they have the same truth value for every choice of $P(x)$, $Q(x)$, and D, or (b) there is a choice of $P(x)$, $Q(x)$, and D for which they have opposite truth values.

55. $\forall x \in D$, $(P(x) \wedge Q(x))$, and

$$(\forall x \in D, P(x)) \wedge (\forall x \in D, Q(x))$$

56. $\exists x \in D, (P(x) \wedge Q(x))$, and
$(\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x))$

57. $\forall x \in D, (P(x) \vee Q(x))$, and
$(\forall x \in D, P(x)) \vee (\forall x \in D, Q(x))$

58. $\exists x \in D, (P(x) \vee Q(x))$, and
$(\exists x \in D, P(x)) \vee (\exists x \in D, Q(x))$

In 59–61, find the answers Prolog would give if the following questions were added to the program given in Example 3.3.11.

59. a. ?isabove(b_1, w_1)
b. ?color(X, white)
c. ?isabove(X, b_3)

60. a. ?isabove(w_1, g)
b. ?color(w_2, blue)
c. ?isabove(X, b_1)

61. a. ?isabove(w_2, b_3)
b. ?color(X, gray)
c. ?isabove(g, X)

ANSWERS FOR TEST YOURSELF

1. an element y in E; y; $P(x, y)$ **2.** an element x in D; y in E; $P(x, y)$ **3.** $\exists x$ such that $\forall y$, the property $P(x, y)$ is false. **4.** $\forall x$, $\exists y$ such that the property $P(x, y)$ is false. **5.** The answer is (c): the truth or falsity of a statement in which the quantifiers are reversed depends on the nature of the property involving x and y.

3.4 Arguments with Quantified Statements

The only complete safeguard against reasoning ill, is the habit of reasoning well; familiarity with the principles of correct reasoning; and practice in applying those principles. —John Stuart Mill

The rule of *universal instantiation* (in-stan-she-AY-shun) says the following:

Universal Instantiation

If a property is true of *everything* in a set, then it is true of *any particular* thing in the set.

Use of the words *universal instantiation* indicates that the truth of a property in a particular case follows as a special instance of its more general or universal truth. The validity of this argument form follows immediately from the definition of truth values for a universal statement. One of the most famous examples of universal instantiation is the following:

All men are mortal.
Socrates is a man.
$\therefore$ Socrates is mortal.

Universal instantiation is *the* fundamental tool of deductive reasoning. Mathematical formulas, definitions, and theorems are like general templates that are used over and over in a wide variety of particular situations. A given theorem says that such and such is true for all things of a certain type. If, in a given situation, you have a particular object of that type, then by universal instantiation, you conclude that such and such is true for that particular object. You may repeat this process 10, 20, or more times in a single proof or problem solution.

As an example of universal instantiation, suppose you are doing a problem that requires you to simplify

$$r^{k+1} \cdot r,$$

where r is a particular real number and k is a particular integer. You know from your study of algebra that the following universal statements are true:

1. For every real number x and for all integers m and n, $x^m \cdot x^n = x^{m+n}$.
2. For every real number x, $x^1 = x$.

So you proceed as follows:

$$\begin{aligned} r^{k+1} \cdot r &= r^{k+1} \cdot r^1 && \text{Step 1} \\ &= r^{(k+1)+1} && \text{Step 2} \\ &= r^{k+2} && \text{by basic algebra.} \end{aligned}$$

Here is the reasoning behind steps 1 and 2.

Step 1: For every real number x, $x^1 = x$. — universal truth
r is a particular real number. — particular instance
$\therefore r^1 = r$. — conclusion

Step 2: For every real number x and for all integers m and n, $x^m \cdot x^n = x^{m+n}$. — universal truth
r is a particular real number and $k+1$ and 1 are particular integers. — particular instance
$\therefore r^{k+1} \cdot r^1 = r^{(k+1)+1}$. — conclusion

Both arguments are examples of universal instantiation.

Universal Modus Ponens

The rule of universal instantiation can be combined with modus ponens to obtain the valid form of argument called *universal modus ponens*.

Universal Modus Ponens

Formal Version	*Informal Version*
$\forall x$, if $P(x)$ then $Q(x)$.	If x makes $P(x)$ true, then x makes $Q(x)$ true.
$P(a)$ for a particular a.	a makes $P(x)$ true.
$\therefore Q(a)$.	$\therefore a$ makes $Q(x)$ true.

Note that the first, or major, premise of universal modus ponens could be written "All things that make $P(x)$ true make $Q(x)$ true," in which case the conclusion would follow by universal instantiation alone. However, the if-then form is more natural to use in the majority of mathematical situations.

Example 3.4.1 **Recognizing Universal Modus Ponens**

Rewrite the following argument using quantifiers, variables, and predicate symbols. Is this argument valid? Why?

If an integer is even, then its square is even.
k is a particular integer that is even.
$\therefore k^2$ is even.

Solution The major premise of this argument can be rewritten as

$\forall x$, if x is an even integer then x^2 is even.

Let $E(x)$ be "x is an even integer," let $S(x)$ be "x^2 is even," and let k stand for a particular integer that is even. Then the argument has the following form:

$\forall x$, if $E(x)$ then $S(x)$.
$E(k)$, for a particular k.
$\therefore S(k)$.

This argument has the form of universal modus ponens and is therefore valid. ■

Example 3.4.2 **Drawing Conclusions Using Universal Modus Ponens**

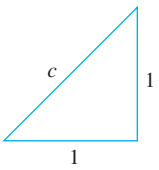
Write the conclusion that can be inferred using universal modus ponens.

If T is any right triangle with hypotenuse c and legs a and b, then $c^2 = a^2 + b^2$.

The triangle shown at the right is a right triangle with both legs equal to 1 and hypotenuse c.

$\therefore$ _____

Pythagorean Theorem



Solution $c^2 = 1^2 + 1^2 = 2$

Note that if you take the nonnegative square root of both sides of this equation, you obtain $c = \sqrt{2}$. This shows that there is a line segment whose length is $\sqrt{2}$. Section 4.7 contains a proof that $\sqrt{2}$ is not a rational number. ■

Use of Universal Modus Ponens in a Proof

In Chapter 4 we discuss methods of proving quantified statements. Here is a proof that the sum of any two even integers is even. It makes use of the definition of even integer, namely, that an integer is *even* if, and only if, it equals twice some integer. (Or, more formally: $\forall$ integers x, x is even if, and only if, $\exists$ an integer—say, k—such that $x = 2k$.)

Suppose m and n are particular but arbitrarily chosen even integers. Then $m = 2r$ for some integer r,(1) and $n = 2s$ for some integer s.(2) Hence

$$\begin{aligned} m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s)^{(3)} && \text{by factoring out the 2.} \end{aligned}$$

Now $r + s$ is an integer,(4) and so $2(r + s)$ is even.(5) Thus $m + n$ is even.

The following expansion of the proof shows how each of the numbered steps is justified by arguments that are valid by universal modus ponens.

Note The logical principle of **existential instantiation** says that if we know or have deduced that something exists, we may give it a name. This is the principle that allows us to call the integers r and s.

(1) If an integer is even, then it equals twice some integer.
m is a particular even integer.
$\therefore$ m equals twice some integer, say, r.

(2) If an integer is even, then it equals twice some integer.
n is a particular even integer.
$\therefore$ n equals twice some integer, say, s.

(3) If a quantity is an integer, then it is a real number.
r and s are particular integers.
$\therefore$ r and s are real numbers.

For all a, b, and c, if a, b, and c are real numbers, then $ab + ac = a(b + c)$.
2, r, and s are particular real numbers.
$\therefore$ $2r + 2s = 2(r + s)$.

(4) For all u and v, if u and v are integers, then $u + v$ is an integer.
r and s are two particular integers.
$\therefore r + s$ is an integer.

(5) If a number equals twice some integer, then that number is even.
$2(r + s)$ equals twice the integer $r + s$.
$\therefore 2(r + s)$ is even.

Of course, the actual proof that the sum of even integers is even does not explicitly contain the sequence of arguments given above. In fact, people who are good at analytical thinking are normally not even conscious that they are reasoning in this way because they have absorbed the method so completely that it has become almost as automatic as breathing.

Universal Modus Tollens

Another crucially important rule of inference is *universal modus tollens*. Its validity results from combining universal instantiation with modus tollens. Universal modus tollens is the heart of proof of contradiction, which is one of the most important methods of mathematical argument.

Universal Modus Tollens

Formal Version	*Informal Version*
$\forall x$, if $P(x)$ then $Q(x)$.	If x makes $P(x)$ true, then x makes $Q(x)$ true.
$\sim Q(a)$, for a particular a.	a does not make $Q(x)$ true.
$\therefore \sim P(a)$.	$\therefore a$ does not make $P(x)$ true.

Example 3.4.3 **Recognizing the Form of Universal Modus Tollens**

Rewrite the following argument using quantifiers, variables, and predicate symbols. Write the major premise in conditional form. Is this argument valid? Why?

All human beings are mortal.
Zeus is not mortal.
$\therefore$ Zeus is not human.

Solution The major premise can be rewritten as

$\forall x$, if x is human then x is mortal.

Let $H(x)$ be "x is human," let $M(x)$ be "x is mortal," and let Z stand for Zeus. The argument becomes

$\forall x$, if $H(x)$ then $M(x)$
$\sim M(Z)$
$\therefore \sim H(Z)$.

This argument has the form of universal modus tollens and is therefore valid. ■

Example 3.4.4 **Drawing Conclusions Using Universal Modus Tollens**

Write the conclusion that can be inferred using universal modus tollens.

All professors are absent-minded.
Tom Hutchins is not absent-minded.
$\therefore$ _____.

Solution Tom Hutchins is not a professor. ■

Proving Validity of Arguments with Quantified Statements

The intuitive definition of validity for arguments with quantified statements is the same as for arguments with compound statements. An argument is valid if, and only if, the truth of its conclusion follows *necessarily* from the truth of its premises. The formal definition is as follows:

Definition

To say that an *argument form* is **valid** means the following: No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true. An *argument* is called **valid** if, and only if, its form is valid. It is called **sound** if, and only if, its form is valid and its premises are true.

As already noted, the validity of universal instantiation follows immediately from the definition of the truth value of a universal statement. General formal proofs of validity of arguments in the predicate calculus are beyond the scope of this book. We give the proof of the validity of universal modus ponens as an example to show that such proofs are possible and to give an idea of how they look.

Universal modus ponens asserts that

$\forall x$, if $P(x)$ then $Q(x)$.
$P(a)$ for a particular a.
$\therefore Q(a)$.

To prove that this form of argument is valid, suppose the major and minor premises are both true. *[We must show that the conclusion "$Q(a)$" is also true.]* By the minor premise, $P(a)$ is true for a particular value of a. By the major premise and universal instantiation, the statement "If $P(a)$ then $Q(a)$" is true for that particular a. But by modus ponens, since the statements "If $P(a)$ then $Q(a)$" and "$P(a)$" are both true, it follows that $Q(a)$ is true also. *[This is what was to be shown.]*

The proof of validity given above is abstract and somewhat subtle. We include the proof not because we expect that you will be able to make up such proofs yourself at this stage of your study. Rather, it is intended as a glimpse of a more advanced treatment of the subject, which you can try your hand at in exercises 35 and 36 at the end of this section if you wish.

One of the paradoxes of the formal study of logic is that the laws of logic are used to prove that the laws of logic are valid!

In the next part of this section we show how you can use diagrams to analyze the validity or invalidity of arguments that contain quantified statements. Diagrams do not provide totally rigorous proofs of validity and invalidity, and in some complex settings they may even be confusing, but in many situations they are helpful and convincing.

Using Diagrams to Test for Validity

Consider the statement

All integers are rational numbers.

Or, formally,

$\forall$ integer n, n is a rational number.

Picture the set of all integers and the set of all rational numbers as disks. The truth of the given statement is represented by placing the integers disk entirely inside the rationals disk, as shown in Figure 3.4.1.

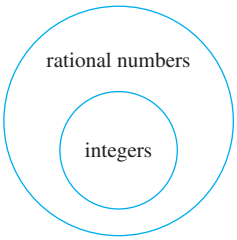


FIGURE 3.4.1

Bettmann/Getty Images

G. W. Leibniz (1646–1716)

Because the two statements "$\forall x \in D$, $Q(x)$" and "$\forall x$, if x is in D then $Q(x)$" are logically equivalent, both can be represented by diagrams like the foregoing.

Perhaps the first person to use diagrams like these to analyze arguments was the German mathematician and philosopher Gottfried Wilhelm Leibniz. Leibniz (LIPE-nits) was far ahead of his time in anticipating modern symbolic logic. He also developed the main ideas of the differential and integral calculus at approximately the same time as (and independently of) Isaac Newton (1642–1727).

To test the validity of an argument diagrammatically, represent the truth of both premises with diagrams. Then analyze the diagrams to see whether they necessarily represent the truth of the conclusion as well.

Example 3.4.5 **Using a Diagram to Show Validity**

Use diagrams to show the validity of the following syllogism:

All human beings are mortal.

Zeus is not mortal.

$\therefore$ Zeus is not a human being.

Solution The major premise is pictured on the left in Figure 3.4.2 by placing a disk labeled "human beings" inside a disk labeled "mortals." The minor premise is pictured on the right in Figure 3.4.2 by placing a dot labeled "Zeus" outside the disk labeled "mortals."

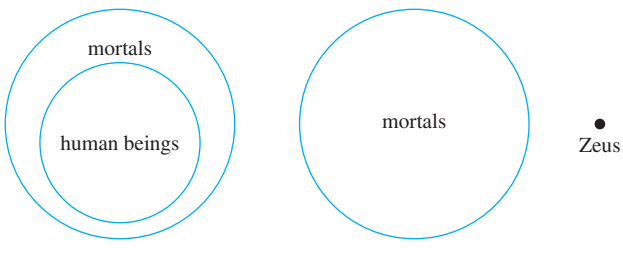


FIGURE 3.4.2

The two diagrams fit together in only one way, as shown in Figure 3.4.3.

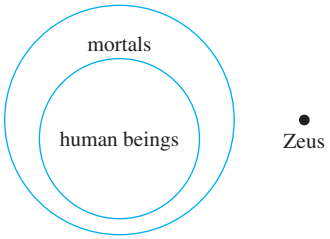


FIGURE 3.4.3

Since the Zeus dot is outside the mortals disk, it is necessarily outside the human beings disk. Thus the truth of the conclusion follows necessarily from the truth of the premises. It is impossible for the premises of this argument to be true and the conclusion false; hence the argument is valid. ■

Example 3.4.6 **Using Diagrams to Show *In*validity**

Use a diagram to show the invalidity of the following argument:

All human beings are mortal.
Felix is mortal.
∴ Felix is a human being.

Solution The major and minor premises are represented diagrammatically in Figure 3.4.4.

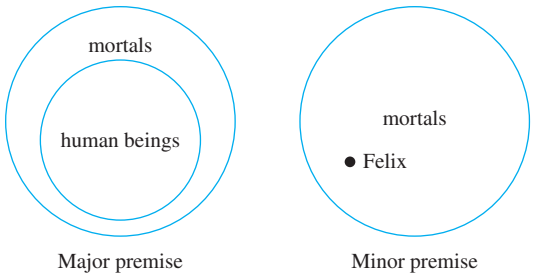


FIGURE 3.4.4

All that is known is that the Felix dot is located *somewhere* inside the mortals disk. Where it is located with respect to the human beings disk cannot be determined. Either one of the situations shown in Figure 3.4.5 might be the case.

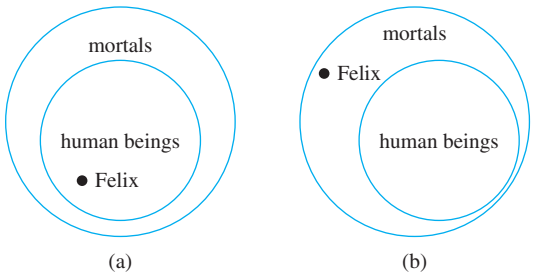


FIGURE 3.4.5

Caution! Be careful when using diagrams to test for validity! For instance, in this example if you put the diagrams for the premises together to obtain only Figure 3.4.5(a) and not Figure 3.4.5(b), you would conclude erroneously that the argument was valid.

The conclusion "Felix is a human being" is true in the first case but not in the second (Felix might, for example, be a cat). Because the conclusion does not necessarily follow from the premises, the argument is invalid. ■

The argument of Example 3.4.6 would be valid if the major premise were replaced by its converse. But since a universal conditional statement is not logically equivalent to its converse, such a replacement cannot, in general, be made. We say that this argument exhibits the converse error.

Converse Error (Quantified Form)

Formal Version	*Informal Version*
$\forall x$, if $P(x)$ then $Q(x)$.	If x makes $P(x)$ true, then x makes $Q(x)$ true.
$Q(a)$ for a particular a.	a makes $Q(x)$ true.
$\therefore P(a)$. ← invalid conclusion	$\therefore a$ makes $P(x)$ true. ← invalid conclusion

The following form of argument would be valid if a conditional statement were logically equivalent to its inverse. But it is not, and the argument form is invalid. We say that it exhibits the inverse error. You are asked to show the invalidity of this argument form in the exercises at the end of this section.

Inverse Error (Quantified Form)

Formal Version	*Informal Version*
$\forall x$, if $P(x)$ then $Q(x)$.	If x makes $P(x)$ true, then x makes $Q(x)$ true.
$\sim P(a)$, for a particular a.	a does not make $P(x)$ true.
$\therefore \sim Q(a)$. ← invalid conclusion	$\therefore a$ does not make $Q(x)$ true. ← invalid conclusion

Example 3.4.7 **An Argument with "No"**

Use diagrams to test the following argument for validity:

No polynomial functions have horizontal asymptotes.
This function has a horizontal asymptote.
∴ This function is not a polynomial function.

Solution A good way to represent the major premise diagrammatically is shown in Figure 3.4.6, two disks—a disk for polynomial functions and a disk for functions with horizontal asymptotes—that do not overlap at all. The minor premise is represented by placing a dot labeled "this function" inside the disk for functions with horizontal asymptotes.

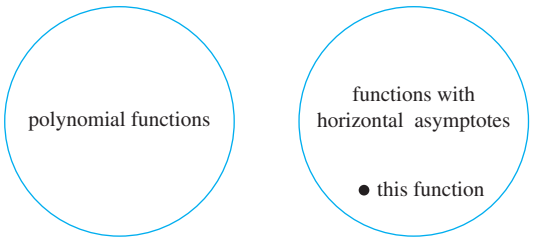


FIGURE 3.4.6

The diagram shows that "this function" must lie outside the polynomial functions disk, and so the truth of the conclusion necessarily follows from the truth of the premises. Hence the argument is valid. ■

An alternative way to solve Example 3.4.7 is to transform "No polynomial functions have horizontal asymptotes" into the equivalent statement "$\forall x$, if x is a polynomial function, then x does not have a horizontal asymptote." If this is done, the argument can be seen to have the form

$$\begin{aligned} &\forall x, \text{ if } P(x) \text{ then } Q(x). \\ &\sim Q(a), \text{ for a particular } a. \\ \therefore\ &\sim P(a). \end{aligned}$$

where $P(x)$ is "x is a polynomial function" and $Q(x)$ is "x does not have a horizontal asymptote." This is valid by universal modus tollens.

Creating Additional Forms of Argument

Universal modus ponens and modus tollens were obtained by combining universal instantiation with modus ponens and modus tollens. In the same way, additional forms of arguments involving universally quantified statements can be obtained by combining universal instantiation with other of the valid argument forms given in Section 2.3. For instance, in Section 2.3 the argument form called transitivity was introduced:

$$\begin{aligned} &p \to q \\ &q \to r \\ \therefore\ &p \to r \end{aligned}$$

This argument form can be combined with universal instantiation to obtain the following valid argument form.

Universal Transitivity

Formal Version	*Informal Version*
$\forall x\ P(x) \to Q(x).$	Any x that makes $P(x)$ true makes $Q(x)$ true.
$\forall x\ Q(x) \to R(x).$	Any x that makes $Q(x)$ true makes $R(x)$ true.
$\therefore \forall x\ P(x) \to R(x).$	$\therefore$ Any x that makes $P(x)$ true makes $R(x)$ true.

Example 3.4.8 **Evaluating an Argument for Tarski's World**

The following argument refers to the kind of arrangement of objects of various types and colors described in Examples 3.1.13 and 3.3.1. Reorder and rewrite the premises to show that the conclusion follows as a valid consequence from the premises.

1. All the triangles are blue.
2. If an object is to the right of all the squares, then it is above all the circles.
3. If an object is not to the right of all the squares, then it is not blue.

$\therefore$ All the triangles are above all the circles.

Solution It is helpful to begin by rewriting the premises and the conclusion in if-then form:

1. $\forall x$, if x is a triangle, then x is blue.
2. $\forall x$, if x is to the right of all the squares, then x is above all the circles.

3. $\forall x$, if x is not to the right of all the squares, then x is not blue.

$\therefore \forall x$, if x is a triangle, then x is above all the circles.

The goal is to reorder the premises so that the conclusion of each is the same as the hypothesis of the next. Also, the hypothesis of the argument's conclusion should be the same as the hypothesis of the first premise, and the conclusion of the argument's conclusion should be the same as the conclusion of the last premise. To achieve this goal, it may be necessary to rewrite some of the statements in contrapositive form.

In this example you can see that the first premise should remain where it is, but the second and third premises should be interchanged. Then the hypothesis of the argument is the same as the hypothesis of the first premise, and the conclusion of the argument's conclusion is the same as the conclusion of the third premise. But the hypotheses and conclusions of the premises do not quite line up. This is remedied by rewriting the third premise in contrapositive form.

1. $\forall x$, if x is a triangle, then x is blue.

3. $\forall x$, if x is blue, then x is to the right of all the squares.

2. $\forall x$, if x is to the right of all the squares, then x is above all the circles.

Putting 1 and 3 together and using universal transitivity gives that

4. $\forall x$, if x is a triangle, then x is to the right of all the squares.

And putting 4 together with 2 and using universal transitivity gives that

$\therefore \forall x$, if x is a triangle, then x is above all the circles,

which is the conclusion of the argument. ■

Remark on the Converse and Inverse Errors

One reason why so many people make converse and inverse errors is that the forms of the resulting arguments would be valid if the major premise were a biconditional rather than a simple conditional. And, as we noted in Section 2.2, many people tend to conflate biconditionals and conditionals.

Consider, for example, the following argument:

All the town criminals frequent the Den of Iniquity bar.

John frequents the Den of Iniquity bar.

$\therefore$ John is one of the town criminals.

The conclusion of this argument is invalid—it results from making the converse error. Therefore, it may be false even when the premises of the argument are true. This type of argument attempts unfairly to establish guilt by association.

The closer, however, the major premise comes to being a biconditional, the more likely the conclusion is to be true. If hardly anyone but criminals frequent the bar and John also frequents the bar, then it is likely (though not certain) that John is a criminal. On the basis of the given premises, it might be sensible to be suspicious of John, but it would be wrong to convict him.

A variation of the converse error is a very useful reasoning tool, provided that it is used with caution. It is the type of reasoning that is used by doctors to make medical diagnoses and by auto mechanics to repair cars. It is the type of reasoning used to generate explanations for phenomena. It goes like this:

If a statement of the form

For every x, if $P(x)$ then $Q(x)$

is true, and if

$Q(a)$ is true, for a particular a,

then check out the statement $P(a)$; it just might be true. For instance, suppose a doctor knows that

For every x, if x has pneumonia, then x has a fever and chills, coughs deeply, and feels exceptionally tired and miserable.

And suppose the doctor also knows that

John has a fever and chills, coughs deeply, and feels exceptionally tired and miserable.

On the basis of these data, the doctor concludes that a diagnosis of pneumonia is a strong possibility, though not a certainty. The doctor will probably attempt to gain further support for this diagnosis through laboratory testing that is specifically designed to detect pneumonia. Note that the closer a set of symptoms comes to being a necessary and sufficient condition for an illness, the more nearly certain the doctor can be of his or her diagnosis.

This form of reasoning has been named **abduction** by researchers working in artificial intelligence. It is used in certain computer programs, called expert systems, that attempt to duplicate the functioning of an expert in some field of knowledge.

TEST YOURSELF

1. The rule of universal instantiation says that if some property is true for _____ in a domain, then it is true for _____.
2. If the first two premises of universal modus ponens are written as "If x makes $P(x)$ true, then x makes $Q(x)$ true" and "For a particular value of a _____," then the conclusion can be written as "_____."
3. If the first two premises of universal modus tollens are written as "If x makes $P(x)$ true, then x makes $Q(x)$ true" and "For a particular value of a _____," then the conclusion can be written as "_____."
4. If the first two premises of universal transitivity are written as "Any x that makes $P(x)$ true makes $Q(x)$ true" and "Any x that makes $Q(x)$ true makes $R(x)$ true," then the conclusion can be written as "_____."
5. Diagrams can be helpful in testing an argument for validity. However, if some possible configurations of the premises are not drawn, a person could conclude that an argument was _____ when it was actually _____.

EXERCISE SET 3.4

1. Let the following law of algebra be the first statement of an argument: For all real numbers a and b,

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Suppose each of the following statements is, in turn, the second statement of the argument. Use universal instantiation or universal modus ponens to write the conclusion that follows in each case.

a. $a = x$ and $b = y$ are particular real numbers.
b. $a = f_i$ and $b = f_j$ are particular real numbers.
c. $a = 3u$ and $b = 5v$ are particular real numbers.
d. $a = g(r)$ and $b = g(s)$ are particular real numbers.
e. $a = \log(t_1)$ and $b = \log(t_2)$ are particular real numbers.

Use universal instantiation or universal modus ponens to fill in valid conclusions for the arguments in 2–4.

2. If an integer n equals $2 \cdot k$ and k is an integer, then n is even.
   0 equals $2 \cdot 0$ and 0 is an integer.
   $\therefore$ _____.

3. For all real numbers a, b, c, and d, if $b \neq 0$ and $d \neq 0$ then $a/b + c/d = (ad + bc)/bd$.
$a = 2$, $b = 3$, $c = 4$, and $d = 5$ are particular real numbers such that $b \neq 0$ and $d \neq 0$.
$\therefore$ _____.

4. $\forall$ real numbers r, a, and b, if r is positive, then $(r^a)^b = r^{ab}$.
$r = 3$, $a = 1/2$, and $b = 6$ are particular real numbers such that r is positive.
$\therefore$ _____.

Use universal modus tollens to fill in valid conclusions for the arguments in 5 and 6.

5. All irrational numbers are real numbers.
$\frac{1}{0}$ is not a real number.
$\therefore$ _____.

6. If a computer program is correct, then compilation of the program does not produce error messages.
Compilation of this program produces error messages.
$\therefore$ _____.

Some of the arguments in 7–18 are valid by universal modus ponens or universal modus tollens; others are invalid and exhibit the converse or the inverse error. State which are valid and which are invalid. Justify your answers.

7. All healthy people eat an apple a day.
Keisha eats an apple a day.
$\therefore$ Keisha is a healthy person.

8. All freshmen must take a writing course.
Caroline is a freshman.
$\therefore$ Caroline must take a writing course.

9. If a graph has no edges, then it has a vertex of degree zero.
This graph has at least one edge.
$\therefore$ This graph does not have a vertex of degree zero.

10. If a product of two numbers is 0, then at least one of the numbers is 0.
For a particular number x, neither $(2x + 1)$ nor $(x - 7)$ equals 0.
$\therefore$ The product $(2x + 1)(x - 7)$ is not 0.

11. All cheaters sit in the back row.
Monty sits in the back row.
$\therefore$ Monty is a cheater.

12. If an 8-bit two's complement represents a positive integer, then the 8-bit two's complement starts with a 0.
The 8-bit two's complement for this integer does not start with a 0.
$\therefore$ This integer is not positive.

13. For every student x, if x studies discrete mathematics, then x is good at logic.
Tarik studies discrete mathematics.
$\therefore$ Tarik is good at logic.

14. If compilation of a computer program produces error messages, then the program is not correct.
Compilation of this program does not produce error messages.
$\therefore$ This program is correct.

15. Any sum of two rational numbers is rational.
The sum $r + s$ is rational.
$\therefore$ The numbers r and s are both rational.

16. If a number is even, then twice that number is even.
The number $2n$ is even, for a particular number n.
$\therefore$ The particular number n is even.

17. If an infinite series converges, then the terms go to 0.
The terms of the infinite series $\sum_{n=1}^{\infty} \frac{1}{n}$ go to 0.
$\therefore$ The infinite series $\sum_{n=1}^{\infty} \frac{1}{n}$ converges.

18. If an infinite series converges, then its terms go to 0.
The terms of the infinite series $\sum_{n=1}^{\infty} \frac{n}{n+1}$ do not go to 0.
$\therefore$ The infinite series $\sum_{n=1}^{\infty} \frac{n}{n+1}$ does not converge.

19. Rewrite the statement "No good cars are cheap" in the form "$\forall x$, if $P(x)$ then $\sim Q(x)$." Indicate whether each of the following arguments is valid or invalid, and justify your answers.

a. No good car is cheap.
A Rimbaud is a good car.
$\therefore$ A Rimbaud is not cheap.

b. No good car is cheap.
A Simbaru is not cheap.
$\therefore$ A Simbaru is a good car.

c. No good car is cheap.
A VX Roadster is cheap.
$\therefore$ A VX Roadster is not good.

d. No good car is cheap.
An Omnex is not a good car.
$\therefore$ An Omnex is cheap.

20. a. Use a diagram to show that the following argument can have true premises and a false conclusion.

All dogs are carnivorous.
Aaron is not a dog.
∴ Aaron is not carnivorous.

b. What can you conclude about the validity or invalidity of the following argument form? Explain how the result from part (a) leads to this conclusion.

$\forall x$, if $P(x)$ then $Q(x)$.
$\sim P(a)$ for a particular a.
$\therefore \sim Q(a)$.

Indicate whether the arguments in 21–27 are valid or invalid. Support your answers by drawing diagrams.

21. All people are mice.
All mice are mortal.
∴ All people are mortal.

22. All discrete mathematics students can tell a valid argument from an invalid one.
All thoughtful people can tell a valid argument from an invalid one.
∴ All discrete mathematics students are thoughtful.

23. All teachers occasionally make mistakes.
No gods ever make mistakes.
∴ No teachers are gods.

24. No vegetarians eat meat.
All vegans are vegetarian.
∴ No vegans eat meat.

25. No college cafeteria food is good.
No good food is wasted.
∴ No college cafeteria food is wasted.

26. All polynomial functions are differentiable.
All differentiable functions are continuous.
∴ All polynomial functions are continuous.

27. [Adapted from Lewis Carroll.]
Nothing intelligible ever puzzles *me*.
Logic puzzles me.
∴ Logic is unintelligible.

In exercises 28–32, reorder the premises in each of the arguments to show that the conclusion follows as a valid consequence from the premises. It may be helpful to rewrite the statements in if-then form and replace some of them by their contrapositives. Exercises 28–30 refer to the kinds of Tarski worlds discussed in Examples 3.1.13 and 3.3.1. Exercises 31 and 32 are adapted from *Symbolic Logic* by Lewis Carroll.*

28. 1. Every object that is to the right of all the blue objects is above all the triangles.
2. If an object is a circle, then it is to the right of all the blue objects.
3. If an object is not a circle, then it is not gray.
∴ All the gray objects are above all the triangles.

29. 1. All the objects that are to the right of all the triangles are above all the circles.
2. If an object is not above all the black objects, then it is not a square.
3. All the objects that are above all the black objects are to the right of all the triangles.
∴ All the squares are above all the circles.

30. 1. If an object is above all the triangles, then it is above all the blue objects.
2. If an object is not above all the gray objects, then it is not a square.
3. Every black object is a square.
4. Every object that is above all the gray objects is above all the triangles.
∴ If an object is black, then it is above all the blue objects.

31. 1. I trust every animal that belongs to me.
2. Dogs gnaw bones.
3. I admit no animals into my study unless they will beg when told to do so.
4. All the animals in the yard are mine.
5. I admit every animal that I trust into my study.
6. The only animals that are really willing to beg when told to do so are dogs.
∴ All the animals in the yard gnaw bones.

32. 1. When I work a logic example without grumbling, you may be sure it is one I understand.
2. The arguments in these examples are not arranged in regular order like the ones I am used to.
3. No easy examples make my head ache.
4. I can't understand examples if the arguments are not arranged in regular order like the ones I am used to.
5. I never grumble at an example unless it gives me a headache.
∴ These examples are not easy.

*Lewis Carroll, *Symbolic Logic* (New York: Dover, 1958), pp. 118, 120, 123.

In 33 and 34 a single conclusion follows when all the given premises are taken into consideration, but it is difficult to see because the premises are jumbled up. Reorder the premises to make it clear that a conclusion follows logically, and state the valid conclusion that can be drawn. (It may be helpful to rewrite some of the statements in if-then form and to replace some statements by their contrapositives.)

33. 1. No birds except ostriches are at least 9 feet tall.
2. There are no birds in this aviary that belong to anyone but me.
3. No ostrich lives on mince pies.
4. I have no birds less than 9 feet high.

34. 1. All writers who understand human nature are clever.
2. No one is a true poet unless he can stir the human heart.
3. Shakespeare wrote *Hamlet*.
4. No writer who does not understand human nature can stir the human heart.
5. None but a true poet could have written *Hamlet*.

***35.** Derive the validity of universal modus tollens from the validity of universal instantiation and modus tollens.

***36.** Derive the validity of universal form of part (a) of the elimination rule from the validity of universal instantiation and the valid argument called elimination in Section 2.3.

ANSWERS FOR TEST YOURSELF

1. all elements; any particular element in the domain (*Or:* each individual element of the domain) **2.** $P(a)$ is true; $Q(a)$ is true **3.** $Q(a)$ is false; $P(a)$ is false **4.** Any x that makes $P(x)$ true makes $R(x)$ true. **5.** valid; invalid (*Or:* invalid; valid)

CHAPTER 4

ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

The underlying content of this chapter consists of properties of integers (whole numbers), rational numbers (integer fractions), and real numbers. The underlying theme of the chapter is how to determine the truth or falsity of a mathematical statement.

Here is an example involving a concept used frequently in computer science. Given any real number x, the floor of x, or greatest integer in x, denoted $\lfloor x \rfloor$, is the largest integer that is less than or equal to x. On the number line, $\lfloor x \rfloor$ is the integer immediately to the left of x (or equal to x if x is, itself, an integer). Thus $\lfloor 2.3 \rfloor = 2$, $\lfloor 12.99999 \rfloor = 12$, and $\lfloor -1.5 \rfloor = -2$. Consider the following two questions:

1. For any real number x, is $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$?
2. For any real numbers x and y, is $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$?

Take a few minutes to try to answer these questions for yourself.

It turns out that the answer to (1) is yes, whereas the answer to (2) is no. Are these the answers you got? If not, don't worry. In Section 4.6 you will learn the techniques you need to answer these questions and more. If you did get the correct answers, congratulations! You have excellent mathematical intuition. Now ask yourself, "How sure am I of my answers? Were they plausible guesses or absolute certainties? Was there any difference in certainty between my answers to (1) and (2)? Would I have been willing to bet a large sum of money on the correctness of my answers?"

One of the best ways to think of a mathematical proof is as a carefully reasoned argument to convince a skeptical listener (often yourself) that a given statement is true. Imagine the listener challenging your reasoning every step of the way, constantly asking, "Why is that so?" If you can counter every possible challenge, then your proof as a whole will be correct.

As an example, imagine proving to someone not very familiar with mathematical notation that if x is a number with $5x + 3 = 33$, then $x = 6$. You could argue as follows:

> If $5x + 3 = 33$, then $5x + 3$ minus 3 will equal $33 - 3$ because subtracting the same number from two equal quantities gives equal results. But $5x + 3$ minus 3 equals $5x$ because adding 3 to $5x$ and then subtracting 3 just leaves $5x$. Also, $33 - 3 = 30$. Hence $5x = 30$. This means that x is a number which when multiplied by 5 equals 30. But the only number with this property is 6. Therefore, if $5x + 3 = 33$ then $x = 6$.

Of course there are other ways to phrase this proof, depending on the level of mathematical sophistication of the intended reader. In practice, mathematicians often omit reasons for certain steps of an argument when they are confident that the reader can easily supply them. When you are first learning to write proofs, however, it is better to err on the side of supplying too many reasons rather than too few. All too frequently, when even the best mathematicians carefully examine some "details" in their arguments, they discover that those details are actually false. One of the most important reasons for requiring proof in

mathematics is that writing a proof forces us to become aware of weaknesses in our arguments and in the unconscious assumptions we have made.

Sometimes correctness of a mathematical argument can be a matter of life or death. Suppose, for example, that a mathematician is part of a team charged with designing a new type of airplane engine, and suppose that the mathematician is given the job of determining whether the thrust delivered by various engine types is adequate. If you knew that the mathematician was only fairly sure, but not positive, of the correctness of his analysis, would you want to ride in the resulting aircraft?

At a certain point in Lewis Carroll's *Alice in Wonderland* (see exercise 28 in Section 2.2), the March Hare tells Alice to "say what you mean." In other words, if she means a thing, then that is exactly what she should say. In this chapter, perhaps more than in any other mathematics course you have ever taken, you will need to say what you mean. Precision of thought and language is essential to achieve the mathematical certainty that is necessary for you to have complete confidence in your solutions to mathematical problems.

4.1 Direct Proof and Counterexample I: Introduction

Mathematics, as a science, commenced when first someone, probably a Greek, proved propositions about "any" things or about "some" things without specification of definite particular things. —Alfred North Whitehead, 1861–1947

Both discovery and proof are integral parts of problem solving. When you think you have discovered that a certain statement is true, try to figure out why it is true. If you succeed, you will know that your discovery is genuine. Even if you fail, the process of trying will give you insight into the nature of the problem and may lead you to discover that the statement is false. For complex problems, the interplay between discovery and proof is not reserved to the end of the problem-solving process but, rather, is an important part of each step.

Assumptions

- In this text we assume a familiarity with the laws of basic algebra, which are listed in Appendix A.
- We also use the three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$, then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$.
- And we use the principle of substitution: For all objects A and B, if $A = B$, then we may substitute B wherever we have A.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.

Note Most quotients of integers are not integers. For example, $3 \div 2$, which equals $3/2$, is not an integer, and $3 \div 0$ is not even a number.

The mathematical content of this section primarily concerns even and odd integers and prime and composite numbers.

Even, Odd, Prime, and Composite Integers

In order to evaluate the truth or falsity of a statement, you must understand what the statement is about. In other words, you must know the meanings of all terms that occur in

the statement. Mathematicians define terms very carefully and precisely and consider it important to learn definitions virtually word for word.

Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, for any integer, n

$$n \text{ is even} \iff n = 2k \text{ for some integer } k$$
$$n \text{ is odd} \iff n = 2k + 1 \text{ for some integer } k$$

It follows from the definition that if you are doing a problem in which you know that a particular integer is even, you can deduce that it has the form $2 \cdot$(some integer). Conversely, if you know that an integer equals $2 \cdot$(some integer), then you can deduce that the integer is even.

Know a particular integer n is even. $\xrightarrow{\text{deduce}}$ n has the form $2 \cdot$(some integer).

Know n has the form $2 \cdot$(some integer). $\xrightarrow{\text{deduce}}$ n is even.

This illustrates why both the *if* and the *only-if* parts of definitions are important in mathematical reasoning. In stating definitions, however, mathematics books often replace the words *if-and-only-if* by the single word *if*, perhaps to seem less formal. For instance, the definition of even might be given as "An integer is even if it equals twice some integer." But when the definition is actually used in a proof, both the *if* and the *only-if* parts are usually needed. So, even when the *only-if* part of a definition is not stated explicitly, you are supposed to understand intuitively that it should be included.

Also observe that the definitions of even and odd integers are quantified statements. In Section 3.1 we pointed out that variables used in quantified statements are local, which means that they are bound by the quantifier to which they are attached and that their scopes extend only to the end of the quantified statements that contain them. As a result, the particular names used for the variables have no meaning themselves and are freely replaceable by other names. For example, you can substitute any symbols you like in place of n and k in the definitions of even and odd without changing the meaning of the definitions.

For every integer n, n is *even* if, and only if, $n = 2r$ for some integer r.

For every integer m, m is *even* if, and only if, $m = 2a$ for some integer a.

For every integer a, a is *odd* if, and only if, $a = 2s + 1$ for some integer s.

For every integer k, k is *odd* if, and only if, $k = 2n + 1$ for some integer n.

Example 4.1.1 **Even and Odd Integers**

Use the definitions of *even* and *odd* to justify your answers to the following questions.

a. Is 0 even?

b. Is -301 odd?

c. If a and b are integers, is $6a^2b$ even?

d. If a and b are integers, is $10a + 8b + 1$ odd?

e. Is every integer either even or odd?

Solution

a. Yes, 0 is even because $0 = 2 \cdot 0$.

b. Yes, -301 is odd because $-301 = 2(-151) + 1$ and -151 is an integer.

c. Yes, $6a^2b$ is even because $6a^2b = 2(3a^2b)$ and $3a^2b$ is an integer since it is a product of integers.

d. Yes, $10a + 8b + 1$ is odd because $10a + 8b + 1 = 2(5a + 4b) + 1$ and $5a + 4b$ is an integer since it is a sum of products of integers.

e. Yes, every integer is either even or odd. However, the reason for this fact is not immediately apparent. It can be deduced using the method of proof by contradiction, which is introduced in Section 4.7. It is also a consequence of the quotient-remainder theorem, which is stated in Section 4.5. ■

The integer 6, which equals $2 \cdot 3$, is a product of two smaller positive integers. On the other hand, 7 cannot be written as a product of two smaller positive integers; its only positive factors are 1 and 7. A positive integer, such as 7, that cannot be written as a product of two smaller positive integers is called *prime*.

Definition

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols: For each integer n with $n > 1$,

$$n \text{ is prime} \iff \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1.$$

$$n \text{ is composite} \iff \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n.$$

Example 4.1.2 **Prime and Composite Numbers**

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

Solution

Note The reason for not allowing 1 to be prime is discussed in Section 4.4.

a. No. A prime number is required to be greater than 1.

b. Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely, $r = n$ and $s = 1$ and $r = 1$ and $s = n$. Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \leq r \leq n$ and $1 \leq s \leq n$. If n is prime, then these two pairs are the only ways to write n as rs. Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

c. 2, 3, 5, 7, 11, 13

d. 4, 6, 8, 9, 10, 12 ■

Proving Existential Statements

According to the definition given in Section 3.1, a statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if, and only if,

$$Q(x) \text{ is true for at least one } x \text{ in } D.$$

One way to prove this is to find an x in D that makes $Q(x)$ true. Another way is to give a set of directions for finding such an x. Both of these methods are called **constructive proofs of existence**. The logical principle underlying such a proof is called **existential generalization**. It says that if you know a certain property is true for a particular object, then you may conclude that "there exists an object for which the property is true."

Example 4.1.3 **Constructive Proofs of Existence**

a. Prove: $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.

b. Suppose that r and s are integers. Prove: $\exists$ an integer k such that $22r + 18s = 2k$.

Solution

a. Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers. Thus $\exists$ an even integer—namely, 10—that can be written in two ways as a sum of two prime numbers.

b. Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers, and by substitution, and the distributive law of algebra,

$$2k = 2(11r + 9s) = 22r + 18s.$$

Thus $\exists$ an integer, namely k, such that $22r + 18s = 2k$. ■

A **nonconstructive proof of existence** involves showing either (a) that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem or (b) that the assumption that there is no such x leads to a contradiction. The disadvantage of a nonconstructive proof is that it may give virtually no clue about where or how x may be found. The widespread use of digital computers in recent years has led to some dissatisfaction with this aspect of nonconstructive proofs and to increased efforts to produce constructive proofs containing directions for computer calculation of the quantity in question.

Disproving Universal Statements by Counterexample

To disprove a statement means to show that it is false. Consider the question of disproving a statement of the form

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

$$\exists x \text{ in } D \text{ such that } P(x) \text{ and not } Q(x).$$

But to show that an existential statement is true, we generally give an example, and because the example is used to show that the original statement is false, we call it a *counterexample*. Thus the method of disproof by *counterexample* can be written as follows:

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample**.

Example 4.1.4 **Disproof by Counterexample**

Disprove the following statement by finding a counterexample:

$$\forall \text{ real numbers } a \text{ and } b, \text{ if } a^2 = b^2 \text{ then } a = b.$$

Solution To disprove this statement, you need to find real numbers a and b such that the hypothesis $a^2 = b^2$ is true and the conclusion $a = b$ is false. The fact that both positive and negative integers have positive squares helps in the search. If you flip through some possibilities in your mind, you will quickly see that 1 and -1 will work (or 2 and -2, or 0.5 and -0.5, and so forth). You only need one such pair to give a counterexample.

Statement: $\forall$ real numbers a and b, if $a^2 = b^2$, then $a = b$.

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, and so $a^2 = b^2$. But $a \neq b$ since $1 \neq -1$.

■

Note Example 4.1.4 shows that it is not always true that if the squares of two numbers are equal, then the numbers are equal. However, it is true that if the squares of two *positive* numbers are equal, then the numbers are equal.

After observing that a property holds in a large number of cases, you may guess that it holds in all cases. You may, however, run into difficulty when you try to prove your guess. Perhaps you just have not figured out the key to the proof, or perhaps your guess is false. Consequently, when you are having serious difficulty proving a general statement, you should interrupt your efforts to look for a counterexample. Analyzing the kinds of problems you are encountering in your proof efforts may help in the search. It may even happen that if you find a counterexample and therefore prove the statement false, your understanding may be sufficiently clarified so that you can formulate a more limited but true version of the statement by changing the hypothesis.

Proving Universal Statements

The vast majority of mathematical statements to be proved are universal. In discussing how to prove such statements, it is helpful to imagine them in a standard form:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

Sections 1.1 and 3.1 give examples showing how to write any universal statement in this form. When D is finite or when only a finite number of elements satisfy $P(x)$, such a statement can be proved by the method of exhaustion.

Example 4.1.5 **The Method of Exhaustion**

Use the method of exhaustion to prove the following statement:

> $\forall n \in \mathbf{Z}$, if n is even and $4 \le n \le 26$ then n can be written as a sum of two prime numbers.

Solution

$$4 = 2+2 \qquad 6 = 3+3 \qquad 8 = 3+5 \qquad 10 = 5+5$$
$$12 = 5+7 \qquad 14 = 11+3 \qquad 16 = 5+11 \qquad 18 = 7+11$$
$$20 = 7+13 \qquad 22 = 5+17 \qquad 24 = 5+19 \qquad 26 = 7+19$$

■

In most mathematical situations, however, the method of exhaustion cannot be used. For instance, to prove by exhaustion that *every* even integer greater than 2 can be written as a sum of two prime numbers you would have to check every even integer. But this is impossible because there are infinitely many such numbers.

Even when the domain is finite, it may be infeasible to use the method of exhaustion. Imagine, for example, trying to check by exhaustion that the multiplication circuitry of a particular computer gives the correct result for every pair of numbers in the computer's range. Since a typical computer would require thousands of years just to compute all possible products of all numbers in its range (not to mention the time it would take to check the accuracy of the answers), checking correctness by the method of exhaustion is obviously impractical.

The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified. It is based on a logical principle sometimes called *universal generalization*. A more descriptive name is *generalizing from the generic particular.*

Generalizing from the Generic Particular

To show that *every* element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

The principle of generalizing from the generic particular is not a typical part of everyday reasoning. Its main use is to determine that a general mathematical statement is correct. The example below introduces the idea.

Example 4.1.6 **Generalizing from the Generic Particular**

At some time you may have been shown a "mathematical trick" like the following. You ask a person to pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number. Then you astound the person by announcing that their final result was 7. How does this "trick" work? Imagine that an empty box ☐ contains whatever number the person picked. The table shows that by the end of the calculations, whatever was in the empty box was subtracted out of the answer.

Step	Visual Result	Algebraic Result
Pick a number.	□	x
Add 5.	□ | | | | |	$x + 5$
Multiply by 4.	□ | | | | | □ | | | | | □ | | | | | □ | | | | |	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	□ | | □ | | □ | | | | | □ | | | | |	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	□ | | □ | | | | |	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	| | | | | | |	$(2x + 7) - 2x = 7$

The x in the table above is another way of holding a place for the number the person picked. It is *particular* (because it is a single object), but it is also *arbitrarily chosen* or *generic* (because any number whatsoever can be put in its place). So you can generalize from the generic particular to conclude that if you follow the steps you will always get 7, regardless of the initial value you put in place of x or inside the empty box. ■

The point of having x be arbitrarily chosen (or generic) is to make a proof that can be generalized to all elements of the domain. By choosing x arbitrarily, you are making no special assumptions about x that are not also true of all other elements of the domain. The word *generic* means "sharing all the common characteristics of a group or class." Thus everything you deduce about a generic element x of the domain is equally true of any other element of the domain.

When the method of generalizing from the generic particular is applied to a property of the form "If $P(x)$ then $Q(x)$," the result is the method of *direct proof.* Recall that the only way an if-then statement can be false is for the hypothesis to be true and the conclusion to be false. Thus, given the statement "If $P(x)$ then $Q(x)$," if you can show that the truth of $P(x)$ compels the truth of $Q(x)$, then you will have proved the statement. It follows by the method of generalizing from the generic particular that to show that "$\forall x$, if $P(x)$ then $Q(x)$," is true for *every* element x in a set D, you suppose x is a particular but arbitrarily chosen element of D that makes $P(x)$ true, and then you show that x makes $Q(x)$ true.

Method of Direct Proof

1. Express the statement to be proved in the form "For every $x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example 4.1.7 **A Direct Proof of a Theorem**

Prove that the sum of any two even integers is even.

Caution! The word *two* in this statement does not necessarily refer to two distinct integers. If a choice of integers is made arbitrarily, the integers are very likely to be distinct, but they might be the same.

Solution Whenever you are presented with a statement to be proved, it is a good idea to ask yourself whether you believe it to be true. In this case you might imagine some pairs of even integers—say $2+4$, $6+10$, $12+12$, $28+54$—and mentally check that their sums are even. However, since you cannot possibly check all pairs of even numbers, you cannot know for sure that the statement is true in general by checking its truth in these particular instances. Many properties hold for a large number of examples and yet fail to be true in general.

To prove this statement in general, you need to show that no matter what even integers are given, their sum is even. But given any two even integers, it is possible to represent them as $2r$ and $2s$ for some integers r and s. And by the distributive law of algebra, $2r+2s = 2(r+s)$, which is even because $r+s$ is an integer. Thus the statement is true in general.

Suppose the statement to be proved is much more complicated than this. What method can you use to derive a proof? You can begin by expressing the statement formally.

Formal Restatement: $\forall$ integers m and n, if m and n are even then $m+n$ is even.

This statement is universally quantified over an infinite domain. Thus to prove it in general, you need to show that no matter what two integers you might be given, if both of them are even then their sum will also be even.

Next ask yourself, "How should I start the proof?" or "What am I supposing?" The answer to such a question gives you the starting point, or first sentence, of the proof.

Starting Point: Suppose m and n are any particular but arbitrarily chosen integers that are even.

Or, in abbreviated form:

Suppose m and n are any even integers.

Then ask yourself, "What conclusion do I need to show in order to complete the proof?"

To Show: $m+n$ is even.

At this point you need to ask yourself, "How do I get from the starting point to the conclusion?" Since both involve the term *even integer*, you must use the definition of this term—and thus you must know what it means for an integer to be even. It follows from the definition that since m and n are even, each equals twice some integer. One of the basic laws of logic, called *existential instantiation*, says, in effect, that if you know something exists, you can give it a name. However, you cannot use the same name to refer to two different things, both of which are currently under discussion.

Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced, then it can be given a name, as long as that name is not currently being used to refer to something else in the same discussion.

Caution! Because m and n are arbitrarily chosen they can be any pair of even integers whatsoever. But if you write $m = 2r$ and $n = 2r$, then m would equal n, which is not usually the case.

Thus since m equals twice some integer, you can give that integer a name, and since n equals twice some integer, you can also give that integer a name:

$$m = 2r, \text{ for some integer } r \qquad \text{and} \qquad n = 2s, \text{ for some integer } s.$$

Now what you want to show is that $m + n$ is even. In other words, you want to show that $m + n$ equals $2 \cdot$(some integer). Having just found alternative representations for m (as $2r$) and n (as $2s$), it seems reasonable to substitute these representations in place of m and n:

$$m + n = 2r + 2s.$$

Your goal is to show that $m + n$ is even. By definition of even, this means that $m + n$ can be written in the form

$$2 \cdot (\text{some integer}).$$

This analysis narrows the gap between the starting point and what is to be shown to showing that

$$2r + 2s = 2 \cdot (\text{some integer}).$$

Why is this true? First, because of the distributive law from algebra, which says that

$$2r + 2s = 2(r + s),$$

and, second, because the sum of any two integers is an integer, which implies that $r + s$ is an integer.

This discussion is summarized by rewriting the statement as a theorem and giving a formal proof of it. (In mathematics, the word *theorem* refers to a statement that is known to be true because it has been proved.) The formal proof, as well as many others in this text, includes explanatory notes to make its logical flow apparent. Such comments are purely a convenience for the reader and could be omitted entirely. For this reason they are italicized and enclosed in italic square brackets: *[ ]*.

Donald Knuth, one of the pioneers of the science of computing, has compared constructing a computer program from a set of specifications to writing a mathematical proof based on a set of axioms.* In keeping with this analogy, the bracketed comments can be thought of as similar to the explanatory documentation provided by a good programmer. Documentation is not necessary for a program to run, but it helps a human reader understand what is going on.

Theorem 4.1.1

The sum of any two even integers is even.

Proof: Suppose m and n are any *[particular but arbitrarily chosen]* even integers. *[We must show that $m + n$ is even.]* By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$\begin{aligned} m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s) && \text{by factoring out a 2.} \end{aligned}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence

$$m + n = 2t \quad \text{where } t \text{ is an integer.}$$

It follows by definition of even that $m + n$ is even. *[This is what we needed to show.]*†

Note Introducing t to equal $r + s$ is another use of existential instantiation.

■

*Donald E. Knuth, *The Art of Computer Programming*, 2nd ed., Vol. I (Reading, MA: Addison-Wesley, 1973), p. ix.

†See page 148 for a discussion of the role of universal modus ponens in this proof.

Most theorems, like Theorem 4.1.1, can be analyzed to a point where you realize that as soon as a certain thing is shown, the theorem will be proved. When that thing has been shown, it is natural to end the proof with the words "this is what we needed to show" or "as was to be shown." The Latin words for this are *quod erat demonstrandum*, or Q.E.D. for short. Proofs in older mathematics books end with these initials.

Note that both the *if* and the *only if* parts of the definition of even were used in the proof of Theorem 4.1.1. Since m and n were known to be even, the *only if* ($\Rightarrow$) part of the definition was used to deduce that m and n had a certain general form. Then, after some algebraic substitution and manipulation, the *if* ($\Leftarrow$) part of the definition was used to deduce that $m + n$ was even.

Getting Proofs Started

Believe it or not, once you understand the idea of generalizing from the generic particular and the method of direct proof, you can write the beginnings of proofs even for theorems you do not understand. The reason is that the starting point and what is to be shown in a proof depend only on the linguistic form of the statement to be proved, not on the content of the statement.

Example 4.1.8 **Identifying the "Starting Point" and the "Conclusion to Be Shown"**

Write the first sentence of a proof (the "starting point") and the last sentence of a proof (the "conclusion to be shown") for the following statement:

Every complete bipartite graph is connected.

Note You are not expected to know anything about complete bipartite graphs.

Solution It is helpful to rewrite the statement formally using a quantifier and a variable:

Formal Restatement: For every (domain) graph G, if (G is complete bipartite) (hypothesis), then (G is connected) (conclusion).

The first sentence, or starting point, of a proof supposes the existence of an object (in this case G) in the domain (in this case the set of all graphs) that satisfies the hypothesis of the if-then part of the statement (in this case that G is complete bipartite). The conclusion to be shown is just the conclusion of the if-then part of the statement (in this case that G is connected).

Starting Point: Suppose G is a *[particular but arbitrarily chosen]* graph such that G is complete bipartite.

Conclusion to Be Shown: G is connected.

Thus the proof has the following shape:

Proof:
Suppose G is a *[particular but arbitrarily chosen]* graph such that G is complete bipartite.
⋮
Therefore, G is connected. ■

Example 4.1.9 **Fill in the Blanks for a Proof**

Fill in the blanks in the proof of the following theorem.

Theorem: For all integers r and s, if r is even and s is odd then $3r + 2s$ is even.

Proof:

Suppose r and s are any *[particular but arbitrarily chosen]* integers such that r is even and s is odd.

[We must show that $3r + 2s$ is even.]

By ___(a)___, $r = 2m$ and $s = 2n + 1$ for some integers m and n.

Then

$$\begin{aligned} 3r + 2s &= 3(2m) + 2(2n + 1) && \text{by } \underline{\text{(b)}} \\ &= 6m + 4n + 2 && \text{by multiplying out} \\ &= 2(3m + 2n + 1) && \text{by factoring out 2} \end{aligned}$$

Let $t = 3m + 2n + 1$.

Then t is an integer because m, n, 3, 2, and 1 are integers and because ___(c)___.

Hence $3r + 2s = 2t$, where t is an integer, and so by ___(d)___, $3r + 2s$ is even *[as was to be shown]*.

Solution

(a) definition of even and odd, (b) substitution, (c) products and sums of integers are integers, (d) definition of even.

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. An integer is even if, and only if, _____.
2. An integer is odd if, and only if, _____.
3. An integer n is prime if, and only if, _____.
4. The most common way to disprove a universal statement is to find _____.
5. According to the method of generalizing from the generic particular, to show that every element of a set satisfies a certain property, suppose x is a _____, and show that _____.
6. To use the method of direct proof to prove a statement of the form, "For every x in a set D, if $P(x)$ then $Q(x)$," one supposes that _____ and one shows that _____.

EXERCISE SET 4.1*

In 1–4 justify your answers by using the definitions of even, odd, prime, and composite numbers.

1. Assume that k is a particular integer.
   - **a.** Is -17 an odd integer?
   - **b.** Is 0 neither even nor odd?
   - **c.** Is $2k - 1$ odd?
2. Assume that c is a particular integer.
   - **a.** Is $-6c$ an even integer?
   - **b.** Is $8c + 5$ an odd integer?
   - **c.** Is $(c^2 + 1) - (c^2 - 1) - 2$ an even integer?
3. Assume that m and n are particular integers.
   - **a.** Is $6m + 8n$ even?
   - **b.** Is $10mn + 7$ odd?
   - **c.** If $m > n > 0$, is $m^2 - n^2$ composite?
4. Assume that r and s are particular integers.
   - **a.** Is $4rs$ even?
   - **b.** Is $6r + 4s^2 + 3$ odd?
   - **c.** If r and s are both positive, is $r^2 + 2rs + s^2$ composite?

Prove the statements in 5–11.

5. There are integers m and n such that $m > 1$ and $n > 1$ and $\frac{1}{m} + \frac{1}{n}$ is an integer.
6. There are distinct integers m and n such that $\frac{1}{m} + \frac{1}{n}$ is an integer.
7. There are real numbers a and b such that
$$\sqrt{a + b} = \sqrt{a} + \sqrt{b}.$$

*For exercises with blue numbers, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or partial solution is given. The symbol * signals that an exercise is more challenging than usual.

8. There is an integer $n > 5$ such that $2^n - 1$ is prime.

9. There is a real number x such that $x > 1$ and $2^x > x^{10}$.

Definition: An integer n is called a **perfect square** if, and only if, $n = k^2$ for some integer k.

10. There is a perfect square that can be written as a sum of two other perfect squares.

11. There is an integer n such that $2n^2 - 5n + 2$ is prime.

In 12–13, (a) write a negation for the given statement, and (b) use a counterexample to disprove the given statement. Explain how the counterexample actually shows that the given statement is false.

12. For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

13. For every integer n, if n is odd then $\frac{n-1}{2}$ is odd.

Disprove each of the statements in 14–16 by giving a counterexample. In each case explain how the counterexample actually disproves the statement.

14. For all integers m and n, if $2m + n$ is odd then m and n are both odd.

15. For every integer p, if p is prime then $p^2 - 1$ is even.

16. For every integer n, if n is even then $n^2 + 1$ is prime.

In 17–20, determine whether the property is true for all integers, true for no integers, or true for some integers and false for other integers. Justify your answers.

17. $(a+b)^2 = a^2 + b^2$

18. $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a+c}{b+d}$

***H* 19.** $-a^n = (-a)^n$

20. The average of any two odd integers is odd.

Prove the statement in 21 and 22 by the method of exhaustion.

21. Every positive even integer less than 26 can be expressed as a sum of three of fewer perfect squares. (For instance, $10 = 1^2 + 3^2$ and $16 = 4^2$.)

22. For each integer n with $1 \le n \le 10$, $n^2 - n + 11$ is a prime number.

Each of the statements in 23–26 is true. For each, (a) rewrite the statement with the quantification implicit as If _____, then _____, and (b) write the first sentence of a proof (the "starting point") and the last sentence of a proof (the "conclusion to be shown"). (Note that you do not need to understand the statements in order to be able to do these exercises.)

23. For every integer m, if $m > 1$ then $0 < \frac{1}{m} < 1$.

24. For every real number x, if $x > 1$ then $x^2 > x$.

25. For all integers m and n, if $mn = 1$ then $m = n = 1$ or $m = n = -1$.

26. For every real number x, if $0 < x < 1$ then $x^2 < x$.

***H* 27.** Fill in the blanks in the following proof.

Theorem: For every odd integer n, n^2 is odd.

Proof: Suppose n is any ___(a)___. By definition of odd, $n = 2k + 1$ for some integer k. Then

$$\begin{aligned} n^2 &= \big(\ \text{(b)}\ \big)^2 && \text{by substitution} \\ &= 4k^2 + 4k + 1 && \text{by multiplying out} \\ &= 2(2k^2 + 2k) + 1 && \text{by factoring out a 2} \end{aligned}$$

Now $2k^2 + 2k$ is an integer because it is a sum of products of integers. Therefore, n^2 equals $2 \cdot$(an integer) $+ 1$, and so ___(c)___ is odd by definition of odd.

Because we have not assumed anything about n except that it is an odd integer, it follows from the principle of ___(d)___ that for *every* odd integer n, n^2 is odd.

In each of 28–31: a. Rewrite the theorem in three different ways: as ∀_____, if _____ then _____, as ∀_____, _____ (without using the words *if* or *then*), and as If _____, then _____ (without using an explicit universal quantifier).

b. Fill in the blanks in the proof of the theorem.

28. Theorem: The sum of any two odd integers is even.

Proof: Suppose m and n are any *[particular but arbitrarily chosen]* odd integers.

[We must show that $m + n$ is even.]

By ___(a)___, $m = 2r + 1$ and $n = 2s + 1$ for some integers r and s.

Then

$$\begin{aligned} m + n &= (2r + 1) + (2s + 1) && \text{by } \text{(b)} \\ &= 2r + 2s + 2 \\ &= 2(r + s + 1) && \text{by algebra.} \end{aligned}$$

Let $u = r + s + 1$. Then u is an integer because r, s, and 1 are integers and because ___(c)___.

Hence $m + n = 2u$, where u is an integer, and so, by __(d)__, $m + n$ is even *[as was to be shown].*

29. Theorem: The negative of any even integer is even.

Proof: Suppose n is any *[particular but arbitrarily chosen]* even integer.

[We must show that $-n$ is even.]

By __(a)__, $n = 2k$ for some integer k.

Then

$$\begin{aligned} -n &= -(2k) && \text{by } \underline{\text{(b)}} \\ &= 2(-k) && \text{by algebra.} \end{aligned}$$

Let $r = -k$. Then r is an integer because (-1) and k are integers and __(c)__.

Hence $-n = 2r$, where r is an integer, and so $-n$ is even by __(d)__ *[as was to be shown].*

30. Theorem 4.1.2: The sum of any even integer and any odd integer is odd.

Proof: Suppose m is any even integer and n is __(a)__. By definition of even, $m = 2r$ for some __(b)__, and by definition of odd, $n = 2s + 1$ for some integer s. By substitution and algebra,

$$m + n = \underline{\text{(c)}} = 2(r + s) + 1.$$

Since r and s are both integers, so is their sum $r + s$. Hence $m + n$ has the form twice some integer plus one, and so __(d)__ by definition of odd.

31. Theorem: Whenever n is an odd integer, $5n^2 + 7$ is even.

Proof: Suppose n is any *[particular but arbitrarily chosen]* odd integer.

[We must show that $5n^2 + 7$ is even.]

By definition of odd, $n =$ __(a)__ for some integer k.

Then

$$\begin{aligned} 5n^2 + 7 &= \underline{\text{(b)}} && \text{by substitution} \\ &= 5(4k^2 + 4k + 1) + 7 \\ &= 20k^2 + 20k + 12 \\ &= 2(10k^2 + 10k + 6) && \text{by algebra.} \end{aligned}$$

Let $t =$ __(c)__. Then t is an integer because products and sums of integers are integers.

Hence $5n^2 + 7 = 2t$, where t is an integer, and thus __(d)__ by definition of even *[as was to be shown].*

ANSWERS FOR TEST YOURSELF

1. it equals twice some integer **2.** it equals twice some integer plus 1 **3.** n is greater than 1 and if n equals the product of any two positive integers, then one of the integers equals 1 and the other equals n. **4.** a counterexample **5.** particular but arbitrarily chosen element of the set; x satisfies the given property **6.** x is a particular but arbitrarily chosen element of the set D that makes the hypothesis $P(x)$ true; x makes the conclusion $Q(x)$ true.

4.2 Direct Proof and Counterexample II: Writing Advice

". . . it is demanded for proof that every doubt becomes impossible." —Carl Friedrich Gauss (1777–1855)

Think of a proof as a way to communicate a convincing argument for the truth of a mathematical statement. When you write a proof, try to be clear and complete. Keep in mind that a classmate reading your proof will see only what you actually write down, not any unexpressed thoughts behind it. Ideally, your proof will lead your reader to understand *why* the given statement is true.

Directions for Writing Proofs of Universal Statements

Over the years, the following rules of style have become fairly standard for writing the final versions of proofs:

1. **Copy the statement of the theorem to be proved on your paper.**
   This makes the theorem statement available for reference to anyone reading the proof.

2. **Clearly mark the beginning of your proof with the word Proof.**
   This word separates general discussion about the theorem from its actual proof.

3. **Make your proof self-contained.**
   This means that you should explain the meaning of each variable used in your proof in the body of the proof. Thus you will begin proofs by introducing the initial variables and stating what kind of objects they are. The first sentence of your proof would be something like "Suppose m and n are any even integers" or "Let x be a real number such that x is greater than 2." This is similar to declaring variables and their data types at the beginning of a computer program.

   At a later point in your proof, you may introduce a new variable to represent a quantity that is known at that point to exist. For example, if you have assumed that a particular integer n is even, then you know that n equals 2 times some integer, and you can give this integer a name so that you can work with it concretely later in the proof. Thus if you decide to call the integer, say, s, you would write, "Since n is even, $n = 2s$ for some integer s," or "since n is even, there exists an integer, say s, such that $n = 2s$."

4. **Write your proof in complete, grammatically correct sentences.**
   This does not mean that you should avoid using symbols and shorthand abbreviations, just that you should incorporate them into sentences. For example, the proof of Theorem 4.1.1 contains the sentence

$$\begin{aligned} \text{Then } m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s) && \text{by factoring out 2.} \end{aligned}$$

   To read such text as a sentence, read the first equals sign as "equals" and each subsequent equals sign as "which equals."

5. **Keep your reader informed about the status of each statement in your proof.**
   Your reader should never be in doubt about whether something in your proof has been assumed or established or is still to be deduced. If something is assumed, preface it with a word like *Suppose* or *Assume*. If it is still to be shown, preface it with words like, *We must show that* or *In other words*, *we must show that*. This is especially important if you introduce a variable in rephrasing what you need to show. (See Common Mistakes on the next page.)

6. **Give a reason for each assertion in your proof.**
   Each assertion in a proof should come directly from the hypothesis of the theorem, or follow from the definition of one of the terms in the theorem, or be a result obtained earlier in the proof, or be a mathematical result that has previously been established or is agreed to be assumed. Indicate the reason for each step of your proof using phrases such as *by hypothesis*, *by definition of . . . by theorem . . .* and so forth.

   It is best to refer to definitions and theorems by name or number. If you need to state one in the body of your proof, avoid using a variable when you write it because otherwise your proof could end up with a variable that has two conflicting meanings.*

   Proofs in more advanced mathematical contexts often omit reasons for some steps because it is assumed that students either understand them or can easily figure them out for themselves. However, in a course that introduces mathematical proof, you should make sure to provide the details of your arguments because you cannot guarantee that your readers have the necessary mathematical knowledge and sophistication to supply them on their own.

*When a variable is used to state a definition, the scope of the variable extends only to the end of the definition. After that, the symbol for the variable no longer has the same meaning. Confusion can result from thinking that the meaning of the symbol continues into other parts of the proof.

7. **Include the "little words and phrases" that make the logic of your arguments clear.**

When writing a mathematical argument, especially a proof, indicate how each sentence is related to the previous one. Does it follow from the previous sentence or from a combination of the previous sentence and earlier ones? If so, start the sentence with the word *Because* or *Since* and state the reason why it follows, or write *Then*, or *Thus*, or *So*, or *Hence*, or *Therefore*, or *Consequently*, or *It follows that*, and include the reason at the end of the sentence. For instance, in the proof of Theorem 4.1.1, once you know that m is even, you can write: "By definition of even, $m = 2r$ for some integer r," or you can write, "Then $m = 2r$ for some integer r by definition of even." And when you write "Then $m + n = 2r + 2s$," add the words *by substitution* to explain why you are allowed to write $2r$ in place of m and $2s$ in place of n.

If a sentence expresses a new thought or fact that does not follow as an immediate consequence of the preceding statement but is needed for a later part of a proof, introduce it by writing *Observe that*, or *Note that*, or *Recall that*, or *But*, or *Now.*

Sometimes in a proof it is desirable to define a new variable in terms of previous variables. In such a case, introduce the new variable with the word *Let*. For instance, in the proof of Theorem 4.1.1, once it is known that $m + n = 2(r + s)$, where r and s are integers, a new variable t is introduced to represent $r + s$. The convention in mathematics and computer science is to put a new variable to the left of the equal sign and the expression that defines it to the right of the sign. Thus the proof goes on to say, "Let $t = r + s$. Then t is an integer because it is a sum of two integers."

8. **Display equations and inequalities.**

The convention is to display equations and inequalities on separate lines to increase readability, both for other people and for ourselves so that we can more easily check our work for accuracy. We follow the convention in the text of this book, but in order to save space, we violate it in a few of the exercises and in many of the solutions contained in Appendix B. So you may need to copy out some parts of solutions on scratch paper to understand them fully. Please follow the convention in your own work. Leave plenty of empty space, and don't be stingy with paper!

Variations among Proofs

It is rare that two proofs of a given statement, written by two different people, are identical. Even when the basic mathematical steps are the same, the two people may use different notation or may give differing amounts of explanation for their steps, or may choose different words to link the steps together into paragraph form. An important question is how detailed to make the explanations for the steps of a proof. This must ultimately be worked out between the writer of a proof and the intended reader, whether they be student and teacher, teacher and student, student and fellow student, or mathematician and colleague. Your teacher may provide explicit guidelines for you to use in your course. Or you may follow the example of the proofs in this book (which are generally explained rather fully in order to be understood by students at various stages of mathematical development). Remember that the phrases written inside brackets *[ ]* are intended to elucidate the logical flow or underlying assumptions of the proof and need not be written down at all. It is your decision whether to include such phrases in your own proofs.

Common Mistakes

The following are some of the most common mistakes people make when writing mathematical proofs.

1. **Arguing from examples.**

Looking at examples is one of the most helpful practices a problem solver can engage in and is encouraged by all good mathematics teachers. However, it is a mistake to think that a general statement can be proved by showing it to be true for some individual cases. A property referred to in a universal statement may be true in many instances without being true in general.

Consider the following "proof" that the sum of any two even integers is even (Theorem 4.1.1).

> This is true because if $m = 14$ and $n = 6$, which are both even,
> then $m + n = 20$, which is also even.

Some people find this kind of argument convincing because it does, after all, consist of evidence in support of a true conclusion. But remember that when we discussed valid arguments, we pointed out that an argument may be invalid and yet have a true conclusion. In the same way, an argument from examples may be mistakenly used to "prove" a true statement. In the previous example, it is not sufficient to show that the conclusion "$m + n$ is even" is true for $m = 14$ and $n = 6$. You must give an argument to show that the conclusion is true for any arbitrarily chosen even integers m and n.

2. **Using the same letter to mean two different things.**

Some beginning theorem provers give a new variable quantity the same letter name as a previously introduced variable. Consider the following "proof" fragment:

> Suppose m and n are any odd integers. Then by definition of odd,
> $m = 2k + 1$ and $n = 2k + 1$ where k is an integer.

You might think of a variable in a mathematical proof as similar to a global variable in a computer program: once introduced, it has the same meaning throughout the program. In other words, its scope extends to the end of the program. In this example, using the symbol k in the expressions for both m and n makes k a global variable. As a result, both m and n equal $2k + 1$, and thus are equal to each other. The proof then only shows that a sum of two identical odd integers is even, not that the sum of two arbitrarily chosen odd integers is even.

3. **Jumping to a conclusion.**

To jump to a conclusion means to allege the truth of something without giving an adequate reason. Consider the following "proof" that the sum of any two even integers is even.

> Suppose m and n are any even integers. By definition of even,
> $m = 2r$ and $n = 2s$ for some integers r and s. Then $m + n = 2r + 2s$.
> So $m + n$ is even.

The problem with this "proof" is that to show an integer is even one needs to show that it equals twice some integer. This proof jumps to the conclusion that $m + n$ is even without having found an integer that, when doubled, equals $m + n$.

4. **Assuming what is to be proved.**

To assume what is to be proved is a variation of jumping to a conclusion. As an example, consider the following "proof" of the fact that the product of any two odd integers is odd:

> Suppose m and n are any odd integers. When any odd integers are
> multiplied, their product is odd. Hence mn is odd.

5. **Confusion between what is known and what is still to be shown.**

A more subtle way to jump to a conclusion occurs when the conclusion is restated using a variable. Here is an example in a "proof" that the product of any two odd integers is odd:

> Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that
>
> $$mn = 2s + 1.$$
>
> Also by definition of odd, there exist integers a and b such that
>
> $$m = 2a + 1 \text{ and } n = 2b + 1.$$
>
> Then
>
> $$mn = (2a + 1)(2b + 1) = 2s + 1.$$
>
> So, since s is an integer, mn is odd by definition of odd.

Note At this point in the proof, we do not know whether there is an integer s making this equality true.

In this example, when the author restated the conclusion to be shown (that mn is odd), the author wrote "there exists an integer s such that $mn = 2s + 1$." But we only know that the integer s exists if we know that mn is odd, which is what the author is trying to show. Thus, in the sentence starting with the word "Then," the author jumped to an unjustified conclusion. This mistake might have been avoided if the author had written

> "This means *we must show that there exists* an integer s such that $mn = 2s + 1$."

Caution! A reader of your proof should never be in doubt about what you have already shown and what still needs to be shown.

An even better way to avoid this kind of error is not to introduce a variable into a proof unless it is either part of the hypothesis or deducible from it.

6. **Use of *any* when the correct word is *some*.**

There are a few situations in which the words *any* and *some* can be used interchangeably. For instance, in starting a proof that the square of any odd integer is odd, one could correctly write, "Suppose m is any odd integer" or "Suppose m is some odd integer." In most situations, however, the words *any* and *some* are not interchangeable. Here is the start of a "proof" that the square of any odd integer is odd, which uses *any* when the correct word is *some*:

> Suppose m is a particular but arbitrarily chosen odd integer.
> By definition of odd, $m = 2a + 1$ for any integer a.

In the second sentence it is incorrect to say that "$m = 2a + 1$ for any integer a" because a cannot be just "any" integer; in fact, solving $m = 2a + 1$ for a shows that the only possible value for a is $(m - 1)/2$. The correct way to finish the second sentence is, "$m = 2a + 1$ for some integer a" or "there exists an integer a such that $m = 2a + 1$."

7. **Misuse of the word *if*.**

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word *if* when the word *because* is really meant. Consider the following proof fragment:

> Suppose p is a prime number. If p is prime, then p cannot be written as a product of two smaller positive integers.

The use of the word *if* in the second sentence is inappropriate. It suggests that the primeness of p is in doubt. But p is known to be prime by the first sentence. It cannot

be written as a product of two smaller positive integers *because* it is prime. Here is a correct version of the fragment:

> Suppose p is a prime number. Because p is prime, p cannot be written as a product of two smaller positive integers.

Example 4.2.1 **An Odd Integer Minus an Even Integer**

Prove that the difference of any odd integer and any even integer is odd. Use only the definitions of odd and even and the Assumptions listed on page 161, not any other properties of odd and even integers. Follow the directions given in this section for writing proofs of universal statements.

Solution

You may already have a sense that the statement to be proved is true, but to make sure your intuition is correct and to develop a careful proof, rewrite the statement using names such as a and b for the odd and even integers so that you will have a convenient way to refer to them:

> For all integers a and b, if a is odd and b is even, then $a - b$ is odd.
>
> *Or:* For every odd integer a and every even integer b, the difference $a - b$ is odd.
>
> *Or:* If a is any odd integer and b is any even integer, then $a - b$ is odd.

Thus the starting point for your proof would be something like, "Suppose a is any odd integer and b is any even integer," and the conclusion to be shown would be "We must show that $a - b$ is odd." If, in addition, you know how to use the definitions of odd and even, you will have reduced the creative part of developing the proof to a small, but crucial, section in the middle.

Theorem 4.2.1

The difference of any odd integer and any even integer is odd.

Proof:

1. Suppose a is any odd integer and b is any even integer. *[We must show that $a - b$ is odd.]*
2. By definition of odd, $a = 2r + 1$ for some integer r, and $b = 2s$ for some integer s.
3. Then $a - b = (2r + 1) - 2s$ by substitution
4. $= 2r - 2s + 1$ by combining like terms
5. $= 2(r - s) + 1$ by factoring out 2.
6. Let $t = r - s$.
7. Then t is an integer because it is a difference of integers.
8. So, by substitution, $a - b = 2t + 1$, where t is an integer.
9. Hence $a - b$ is odd *[as was to be shown]*.

Note that lines 1–3 follow immediately from the general structure of the proof, the definitions of odd and even, and substitution. In order to figure out your next steps, it can be helpful to refer to what must be shown—namely, that $a - b$ is odd. According to the definition of odd, you can conclude that $a - b$ is odd if you can show that it equals $2 \cdot$(some integer) $+ 1$. So showing that $a - b$ is odd involves transforming $(2r + 1) - 2s$ into $2 \cdot$(some integer) $+ 1$. Lines 4–8 show the steps for doing this, and line 9 concludes that what was to be shown has been achieved. ■

Some of the exercises at the end of the section are based on actual student work and ask you to identify mistakes in "proofs" that have been proposed. Example 4.2.2 illustrates the kind of care that must be taken in evaluating a proof.

Example 4.2.2 **Identifying a Mistake in a Proposed Proof**

Find the mistake in the following "proof."

Theorem: If n is any even integer, then $(-1)^n = 1$.

Proof:

1. Suppose n is any even integer. *[We must show that $(-1)^n$ is even.]*
2. By definition of even, $n = 2a$ for some integer a.
3. Then $(-1)^n = (-1)^{2a}$ by substitution
4. $= ((-1)^a)^2$ by a law of exponents
5. $= 1$ because any nonzero real number squared is positive.

Solution

This "proof" incorrectly jumps to a conclusion in line 5. Although it is true that the square of any nonzero real number is positive, it does not follow that the square of $(-1)^a$ is 1. Exercise 10 at the end of this section asks you to give a correct proof of this theorem. ■

Showing That an Existential Statement Is False

Recall that the negation of an existential statement is universal. It follows that to prove an existential statement is false, you must prove a universal statement (its negation) is true.

Example 4.2.3 **Disproving an Existential Statement**

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Solution Proving that the given statement is false is equivalent to proving its negation is true. The negation is

For all positive integers n, $n^2 + 3n + 2$ is not prime.

Because the negation is universal, it is proved by generalizing from the generic particular.

Claim: The statement "There is a positive integer n such that $n^2 + 3n + 2$ is prime" is false.

Proof:

Suppose n is any *[particular but arbitrarily chosen]* positive integer. *[We will show that $n^2 + 3n + 2$ is not prime.]* Factoring shows that

$$n^2 + 3n + 2 = (n + 1)(n + 2).$$

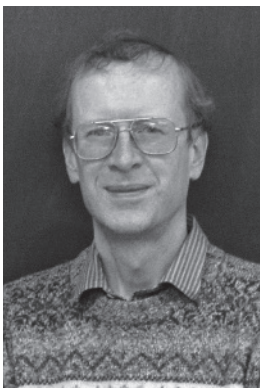
In addition, $n + 1$ and $n + 2$ are integers (because they are sums of integers), and both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$). Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime. ■

Conjecture, Proof, and Disproof

More than 350 years ago, the French mathematician Pierre de Fermat claimed that it is impossible to find positive integers x, y, and z with $x^n + y^n = z^n$ if n is an integer that is at least 3. (For $n = 2$, the equation has many integer solutions, such as $3^2 + 4^2 = 5^2$ and

Bettmann/Getty Images

Pierre de Fermat
(*1601–1665*)



AP Images/Charles Rex Arbogast

Andrew Wiles
(*born 1953*)

$5^2 + 12^2 = 13^2$.) Fermat wrote his claim in the margin of a book, along with the comment "I have discovered a truly remarkable PROOF of this theorem which this margin is too small to contain." No proof, however, was found among his papers, and over the years some of the greatest mathematical minds tried and failed to discover a proof or a counterexample for what came to be known as Fermat's last theorem.

In 1986 Kenneth Ribet of the University of California at Berkeley showed that if a certain other statement, the Taniyama–Shimura conjecture, could be proved, then Fermat's theorem would follow. Andrew Wiles, an English mathematician and faculty member at Princeton University, had become intrigued by Fermat's claim while still a child and, as an adult, had come to work in the branch of mathematics to which the Taniyama–Shimura conjecture belonged. As soon as he heard of Ribet's result, Wiles immediately set to work to prove the conjecture. In June of 1993, after 7 years of concentrated effort, he presented a proof to worldwide acclaim.

During the summer of 1993, however, while the proof was being carefully checked to prepare for publication, Wiles found a step he had difficulty justifying and which he ultimately realized was an error. Having worked alone for so long, he decided to call on a former student, Richard Taylor, then at Cambridge University in England, who agreed to join him in Princeton, and, together, they worked ceaselessly for months to resolve the problem. After almost a year without a breakthrough, Taylor encouraged Wiles to revisit an approach that had been abandoned years earlier, and, as Wiles examined the details, he suddenly saw that the reason it had failed was the exact reason another approach he had previously abandoned would succeed. By the end of 1994, the revised proof had been thoroughly checked and pronounced correct by experts in the field. It was published in the *Annals of Mathematics* in 1995. Several books and an excellent documentary have been produced that convey the drama and excitement of the discovery.*

One of the oldest problems in mathematics that remains unsolved is the Goldbach conjecture. In Example 4.1.5 it was shown that every even integer from 4 to 26 can be represented as a sum of two prime numbers. More than 250 years ago, Christian Goldbach (1690–1764) conjectured that every even integer greater than 2 can be so represented. Explicit computer-aided calculations have shown the conjecture to be true up to at least 10^{18}. But there is a huge chasm between 10^{18} and infinity. As pointed out by James Gleick of the *New York Times*, many other plausible conjectures in number theory have proved false. Leonhard Euler (1707–1783), for example, proposed in the eighteenth century that $a^4 + b^4 + c^4 = d^4$ had no nontrivial whole number solutions. In other words, no three perfect fourth powers add up to another perfect fourth power. For many numbers, Euler's conjecture looked good. But in 1987 a Harvard mathematician, Noam Elkies, proved it wrong. One counterexample, found by Roger Frye of Thinking Machines Corporation in a long computer search, is $95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 422{,}481^4$.†

In May 2000, "to celebrate mathematics in the new millennium," the Clay Mathematics Institute of Cambridge, Massachusetts, announced that it would award prizes of $1 million each for the solutions to seven longstanding, classical mathematical questions. One of them, "P vs. NP," asks whether problems belonging to a certain class can be solved on a computer using more efficient methods than the very inefficient methods that are presently known to work for them. This question is discussed briefly at the end of Chapter 11.

*"The Proof," produced in 1997, for the series *Nova* on the Public Broadcasting System; *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*, by Simon Singh and John Lynch (New York: Bantam Books, 1998); *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem* by Amir D. Aczel (New York: Delacorte Press, 1997).

†James Gleick, "Fermat's Last Theorem Still Has Zero Solutions," *New York Times*, April 17, 1988.

TEST YOURSELF

1. The meaning of every variable used in a proof should be explained within _____.
2. Proofs should be written in sentences that are _____ and _____.
3. Every assertion in a proof should be supported by a _____.
4. The following are some useful "little words and phrases" that clarify the reasoning in a proof: _____, _____, _____, _____, and _____.
5. A new thought or fact that does not follow as an immediate consequence of the preceding statement can be introduced by writing _____, _____, _____, _____, or _____.
6. To introduce a new variable that is defined in terms of previous variables, use the word _____.
7. Displaying equations and inequalities increases the _____ of a proof.
8. Some proof-writing mistakes are _____, _____, _____, _____, _____, _____, and _____.

EXERCISE SET 4.2

Prove the statements in 1–11. In each case use only the definitions of the terms and the Assumptions listed on page 161, not any previously established properties of odd and even integers. Follow the directions given in this section for writing proofs of universal statements.

1. For every integer n, if n is odd then $3n + 5$ is even.
2. For every integer m, if m is even then $3m + 5$ is odd.

H 3. For every integer n, $2n - 1$ is odd.

4. **Theorem 4.2.2:** The difference of any even integer minus any odd integer is odd.
5. If a and b are any odd integers, then $a^2 + b^2$ is even.
6. If k is any odd integer and m is any even integer, then $k^2 + m^2$ is odd.

H 7. The difference between the squares of any two consecutive integers is odd.

8. For any integers m and n, if m is even and n is odd then $5m + 3n$ is odd.
9. If an integer greater than 4 is a perfect square, then the immediately preceding integer is not prime.
10. If n is any even integer, then $(-1)^n = 1$.
11. If n is any odd integer, then $(-1)^n = -1$.

Prove that the statements in 12–14 are false.

12. There exists an integer $m \geq 3$ such that $m^2 - 1$ is prime.
13. There exists an integer n such that $6n^2 + 27$ is prime.
14. There exists an integer $k \geq 4$ such that $2k^2 - 5k + 2$ is prime.

Find the mistakes in the "proofs" shown in 15–19.

15. **Theorem:** For every integer k, if $k > 0$ then $k^2 + 2k + 1$ is composite.

    "**Proof:** For $k = 2$, $k > 0$ and $k^2 + 2k + 1 = 2^2 + 2 \cdot 2 + 1 = 9$. And since $9 = 3 \cdot 3$, then 9 is composite. Hence the theorem is true."

16. **Theorem:** The difference between any odd integer and any even integer is odd.

    "**Proof:** Suppose n is any odd integer, and m is any even integer. By definition of odd, $n = 2k + 1$ where k is an integer, and by definition of even, $m = 2k$ where k is an integer. Then

    $$n - m = (2k + 1) - 2k = 1,$$

    and 1 is odd. Therefore, the difference between any odd integer and any even integer is odd."

17. **Theorem:** For every integer k, if $k > 0$ then $k^2 + 2k + 1$ is composite.

    "**Proof:** Suppose k is any integer such that $k > 0$. If $k^2 + 2k + 1$ is composite, then $k^2 + 2k + 1 = rs$ for some integers r and s such that

    $$1 < r < k^2 + 2k + 1$$

    and

    $$1 < s < k^2 + 2k + 1.$$

    Since

    $$k^2 + 2k + 1 = rs$$

    and both r and s are strictly between 1 and $k^2 + 2k + 1$, then $k^2 + 2k + 1$ is not prime. Hence $k^2 + 2k + 1$ is composite as was to be shown."

18. **Theorem:** The product of any even integer and any odd integer is even.

"**Proof:** Suppose m is any even integer and n is any odd integer. If $m \cdot n$ is even, then by definition of even there exists an integer r such that $m \cdot n = 2r$. Also since m is even, there exists an integer p such that $m = 2p$, and since n is odd there exists an integer q such that $n = 2q + 1$. Thus

$$mn = (2p)(2q + 1) = 2r,$$

where r is an integer. By definition of even, then, $m \cdot n$ is even, as was to be shown."

19. **Theorem:** The sum of any two even integers equals $4k$ for some integer k.

"**Proof:** Suppose m and n are any two even integers. By definition of even, $m = 2k$ for some integer k and $n = 2k$ for some integer k. By substitution,

$$m + n = 2k + 2k = 4k.$$

This is what was to be shown."

In 20–38 determine whether the statement is true or false. Justify your answer with a proof or a counterexample, as appropriate. In each case use only the definitions of the terms and the Assumptions listed on page 161, not any previously established properties.

20. The product of any two odd integers is odd.

H 21. The negative of any odd integer is odd.

22. For all integers a and b, $4a + 5b + 3$ is even.

23. The product of any even integer and any integer is even.

24. If a sum of two integers is even, then one of the summands is even. (In the expression $a + b$, a and b are called **summands**.)

25. The difference of any two even integers is even.

26. For all integers a, b, and c, if a, b, and c are consecutive, then $a + b + c$ is even.

27. The difference of any two odd integers is even.

H 28. For all integers n and m, if $n - m$ is even then $n^3 - m^3$ is even.

29. For every integer n, if n is prime then $(-1)^n = -1$.

30. For every integer m, if $m > 2$ then $m^2 - 4$ is composite.

31. For every integer n, $n^2 - n + 11$ is a prime number.

32. For every integer n, $4(n^2 + n + 1) - 3n^2$ is a perfect square.

33. Every positive integer can be expressed as a sum of three or fewer perfect squares.

H* 34. (Two integers are **consecutive** if, and only if, one is one more than the other.) Any product of four consecutive integers is one less than a perfect square.

35. If m and n are any positive integers and mn is a perfect square, then m and n are perfect squares.

36. The difference of the squares of any two consecutive integers is odd.

H 37. For all nonnegative real numbers a and b, $\sqrt{ab} = \sqrt{a}\sqrt{b}$. (Note that if x is a nonnegative real number, then there is a unique nonnegative real number y, denoted $\sqrt{x}$, such that $y^2 = x$.)

38. For all nonnegative real numbers a and b,

$$\sqrt{a + b} = \sqrt{a} + \sqrt{b}.$$

39. Suppose that integers m and n are perfect squares. Then $m + n + 2\sqrt{mn}$ is also a perfect square. Why?

H* 40. If p is a prime number, must $2^p - 1$ also be prime? Prove or give a counterexample.

*** 41.** If n is a nonnegative integer, must $2^{2n} + 1$ be prime? Prove or give a counterexample.

ANSWERS FOR TEST YOURSELF

1. the body of the proof (or: the proof itself) **2.** complete; grammatically correct **3.** reason **4.** Because; Since; Then; Thus; So; Hence; Therefore; Consequently; It follows that; By substitution **5.** Observe that; Note that; Recall that; But; Now **6.** Let **7.** readability **8.** Arguing from examples; Using the same letter to mean two different things; Jumping to a conclusion; Assuming what is to be proved; Confusion between what is known and what is still to be shown; Use of *any* when the correct word is *some*; Misuse of the word *if*

4.3 Direct Proof and Counterexample III: Rational Numbers

Such, then, is the whole art of convincing. It is contained in two principles: to define all notations used, and to prove everything by replacing mentally the defined terms by their definitions. —Blaise Pascal, 1623–1662

Sums, differences, and products of integers are integers. But most quotients of integers are not integers. Quotients of integers are, however, important; they are known as *rational numbers*.

Definition

A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational**. More formally, if r is a real number, then

$$r \text{ is rational} \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

The word *rational* contains the word *ratio*, which is another word for quotient. A rational number can be written as a ratio of integers.

Example 4.3.1 **Determining Whether Numbers Are Rational or Irrational**

a. Is $10/3$ a rational number?

b. Is $-\frac{5}{39}$ a rational number?

c. Is 0.281 a rational number?

d. Is 7 a rational number?

e. Is 0 a rational number?

f. Is $2/0$ a rational number?

g. Is $2/0$ an irrational number?

h. Is $0.12121212\ldots$ a rational number (where the digits 12 are assumed to repeat forever)?

i. If m and n are integers and neither m nor n is zero, is $(m+n)/mn$ a rational number?

Solution

a. Yes, $10/3$ is a quotient of the integers 10 and 3 and hence is rational.

b. Yes, $-\frac{5}{39} = \frac{-5}{39}$, which is a quotient of the integers -5 and 39 and hence is rational.

c. Yes, $0.281 = 281/1000$. Note that the numbers shown on a typical calculator display are all finite decimals. An explanation similar to the one in this example shows that any such number is rational. It follows that a calculator with such a display can accurately represent only rational numbers.

d. Yes, $7 = 7/1$.

e. Yes, $0 = 0/1$.

f. No, $2/0$ is not a real number (division by 0 is not allowed).

g. No, because every irrational number is a real number, and $2/0$ is not a real number. We discuss additional techniques for determining whether numbers are irrational in Sections 4.7, 4.8, and 7.4.

h. Yes. Let $x = 0.12121212\ldots$ Then $100x = 12.12121212\ldots$ Thus

$$100x - x = 12.12121212\ldots - 0.12121212\ldots = 12.$$

But also $100x - x = 99x$ by basic algebra.

Hence $99x = 12,$

and so $x = \dfrac{12}{99}.$

Therefore, $0.12121212\ldots = 12/99$, which is a ratio of two nonzero integers and thus is a rational number.

Note that you can use an argument similar to this one to show that any repeating decimal is a rational number. In Section 9.4 we show that any rational number can be written as a repeating or terminating decimal.

i. Yes, since m and n are integers, so are $m + n$ and mn (because sums and products of integers are integers). Also $mn \neq 0$ by the *zero product property*. One version of this property says the following:

Zero Product Property

If neither of two real numbers is zero, then their product is also not zero.

(See Theorem T11 in Appendix A and exercise 8 at the end of this section.) It follows that $(m + n)/mn$ is a quotient of two integers with a nonzero denominator and hence is a rational number. ■

More on Generalizing from the Generic Particular

If you claim a property holds for all elements in a domain, then someone can challenge your claim by picking any element in the domain and asking you to prove that that element satisfies the property. To prove your claim, you must be able to meet all such challenges. In other words, you must have a way to convince the challenger that the property is true for an *arbitrarily chosen* element in the domain.

For example, suppose "A" claims that every integer is a rational number. "B" challenges this claim by asking "A" to prove it for $n = 7$. "A" observes that

$$7 = \frac{7}{1} \quad \text{which is a quotient of integers and hence rational.}$$

"B" accepts this explanation but challenges again with $n = -12$. "A" responds that

$$-12 = \frac{-12}{1} \quad \text{which is a quotient of integers and hence rational.}$$

Next "B" tries to trip up "A" by challenging with $n = 0$, but "A" answers that

$$0 = \frac{0}{1} \quad \text{which is a quotient of integers and hence rational.}$$

As you can see, "A" is able to respond effectively to all "B"s challenges because "A" has a general procedure for putting integers into the form of rational numbers: "A" just divides whatever integer "B" gives by 1. That is, no matter what integer n "B" gives "A", "A" writes

$$n = \frac{n}{1} \qquad \text{which is a quotient of integers and hence rational.}$$

This discussion is an informal proof for the following theorem.

Theorem 4.3.1

Every integer is a rational number.

In exercise 11 at the end of this section you are asked to condense the above discussion into a formal proof.

Proving Properties of Rational Numbers

The next example shows how to use the method of generalizing from the generic particular to prove a property of rational numbers.

Example 4.3.2 **Any Sum of Rational Numbers Is Rational**

Prove that the sum of any two rational numbers is rational.

Solution Begin by mentally or explicitly rewriting the statement to be proved in the form "$\forall$ _____, if _____ then _____."

Formal Restatement: $\forall$ real numbers r and s, if r and s are rational then $r + s$ is rational.

Next ask yourself, "Where am I starting from?" or "What am I supposing?" The answer gives you the starting point, or first sentence, of the proof.

Starting Point: Suppose r and s are any particular but arbitrarily chosen real numbers such that r and s are rational; *or, more simply,*

Suppose r and s are any rational numbers.

Then ask yourself, "What must I show to complete the proof?"

To Show: $r + s$ is rational.

Finally ask, "How do I get from the starting point to the conclusion?" or "Why must $r + s$ be rational if both r and s are rational?" The answer depends in an essential way on the definition of rational.

Rational numbers are quotients of integers, so to say that r and s are rational means that

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d} \qquad \text{for some integers } a, b, c, \text{ and } d \text{ where } b \neq 0 \text{ and } d \neq 0.$$

It follows by substitution that

$$r + s = \frac{a}{b} + \frac{c}{d}. \tag{4.3.1}$$

You need to show that $r + s$ is rational, which means that $r + s$ can be written as a single fraction or ratio of two integers with a nonzero denominator. But the right-hand side of equation (4.3.1) is

$$\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} \qquad \text{by rewriting the fraction with a common denominator}$$

$$= \frac{ab + bc}{bd} \qquad \text{by adding fractions with a common denominator.}$$

Is this fraction a ratio of integers? Yes. Because products and sums of integers are integers, $ad + bc$ and bd are both integers. Is the denominator $bd \neq 0$? Yes, by the zero product property (since $b \neq 0$ and $d \neq 0$). Thus $r + s$ is a rational number.

This discussion is summarized as follows:

Theorem 4.3.2

The sum of any two rational numbers is rational.

Proof: Suppose r and s are any rational numbers. *[We must show that $r + s$ is rational.]* Then, by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Thus

$$r + s = \frac{a}{b} + \frac{c}{d} \qquad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \qquad \text{by basic algebra.}$$

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers. Also $q \neq 0$ by the zero product property. Thus

$$r + s = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } q \neq 0.$$

Therefore, $r + s$ is rational by definition of a rational number *[as was to be shown]*.

■

Deriving New Mathematics from Old

Section 4.1 focused on establishing truth and falsity of mathematical theorems using only the basic algebra normally taught in secondary school; the fact that the integers are closed under addition, subtraction, and multiplication; and the definitions of the terms in the theorems themselves. In the future, when we ask you to **prove something directly from the definitions**, we will mean that you should restrict yourself to this approach. However, once a collection of statements has been proved directly from the definitions, another method of proof becomes possible. The statements in the collection can be used to derive additional results.

Example 4.3.3 **Deriving Additional Results about Even and Odd Integers**

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.

3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.
5. The sum of any odd integer and any even integer is odd.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Use the properties listed above to prove that if a is any even integer and b is any odd integer, then $\frac{a^2+b^2+1}{2}$ is an integer.

Solution Suppose a is any even integer and b is any odd integer. By property 3, b^2 is odd, and by property 1, a^2 is even. Then by property 5, a^2+b^2 is odd, and because 1 is also odd, the sum $(a^2+b^2)+1 = a^2+b^2+1$ is even by property 2. Hence, by definition of even, there exists an integer k such that $a^2+b^2+1 = 2k$. Dividing both sides by 2 gives $\frac{a^2+b^2+1}{2} = k$, which is an integer. Thus $\frac{a^2+b^2+1}{2}$ is an integer *[as was to be shown].* ■

A **corollary** is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Example 4.3.4 **The Double of a Rational Number**

Derive the following as a corollary of Theorem 4.3.2.

> **Corollary 4.2.3**
>
> The double of a rational number is rational.

Solution The double of a number is just its sum with itself. But since the sum of any two rational numbers is rational (Theorem 4.3.2), the sum of a rational number with itself is rational. Hence the double of a rational number is rational. Here is a formal version of this argument:

Proof: Suppose r is any rational number. Then $2r = r + r$ is a sum of two rational numbers. So, by Theorem 4.3.2, $2r$ is rational. ■

TEST YOURSELF

1. To show that a real number is rational, we must show that we can write it as _____.
2. An irrational number is a _____ that is _____.
3. Zero is a rational number because _____.

EXERCISE SET 4.3

The numbers in 1–7 are all rational. Write each number as a ratio of two integers.

1. $-\frac{35}{6}$
2. 4.6037
3. $\frac{4}{5}+\frac{2}{9}$
4. 0.37373737 . . .
5. 0.56565656 . . .
6. 320.5492492492 . . .
7. 52.4672167216721 . . .
8. The zero product property, says that if a product of two real numbers is 0, then one of the numbers must be 0.

a. Write this property formally using quantifiers and variables.
b. Write the contrapositive of your answer to part (a).
c. Write an informal version (without quantifier symbols or variables) for your answer to part (b).

9. Assume that a and b are both integers and that $a \neq 0$ and $b \neq 0$. Explain why $(b-a)/(ab^2)$ must be a rational number.

10. Assume that m and n are both integers and that $n \neq 0$. Explain why $(5m-12n)/(4n)$ must be a rational number.

11. Prove that every integer is a rational number.

12. Let S be the statement "The square of any rational number is rational." A formal version of S is "For every rational number r, r^2 is rational." Fill in the blanks in the proof for S.

Proof: Suppose that r is __(a)__. By definition of rational, $r = a/b$ for some __(b)__ with $b \neq 0$. By substitution,

$$r^2 = \text{(c)} = a^2/b^2.$$

Since a and b are both integers, so are the products a^2 and __(d)__. Also $b^2 \neq 0$ by the __(e)__. Hence r^2 is a ratio of two integers with a nonzero denominator, and so __(f)__ by definition of rational.

13. Consider the following statement: The negative of any rational number is rational.
a. Write the statement formally using a quantifier and a variable.
b. Determine whether the statement is true or false and justify your answer.

14. Consider the statement: The cube of any rational number is a rational number.
a. Write the statement formally using a quantifier and a variable.
b. Determine whether the statement is true or false and justify your answer.

Determine which of the statements in 15–19 are true and which are false. Prove each true statement directly from the definitions, and give a counterexample for each false statement. For a statement that is false, determine whether a small change would make it true. If so, make the change and prove the new statement. Follow the directions for writing proofs on page 173.

15. The product of any two rational numbers is a rational number.

***H* 16.** The quotient of any two rational numbers is a rational number.

***H* 17.** The difference of any two rational numbers is a rational number.

***H* 18.** If r and s are any two rational numbers, then $\frac{r+s}{2}$ is rational.

***H* 19.** For all real numbers a and b, if $a < b$ then $a < \frac{a+b}{2} < b$.

(You may use the properties of inequalities in T17–T27 of Appendix A.)

20. Use the results of exercises 18 and 19 to prove that given any two rational numbers r and s with $r < s$, there is another rational number between r and s. An important consequence is that there are infinitely many rational numbers in between any two distinct rational numbers. See Section 7.4.

Use the properties of even and odd integers that are listed in Example 4.3.3 to do exercises 21–23. Indicate which properties you use to justify your reasoning.

21. True or false? If m is any even integer and n is any odd integer, then $m^2 + 3n$ is odd. Explain.

22. True or false? If a is any odd integer, then $a^2 + a$ is even. Explain.

23. True or false? If k is any even integer and m is any odd integer, then $(k+2)^2 - (m-1)^2$ is even. Explain.

Derive the statements in 24–26 as corollaries of Theorems 4.3.1, 4.3.2, and the results of exercises 12, 13, 14, 15, and 17.

24. For any rational numbers r and s, $2r + 3s$ is rational.

25. If r is any rational number, then $3r^2 - 2r + 4$ is rational.

26. For any rational number s, $5s^3 + 8s^2 - 7$ is rational.

27. It is a fact that if n is any nonnegative integer, then

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = \frac{1 - \left(1/2^{n+1}\right)}{1 - (1/2)}.$$

(A more general form of this statement is proved in Section 5.2.) Is the right-hand side of this equation rational? If so, express it as a ratio of two integers.

28. Suppose a, b, c, and d are integers and $a \neq c$. Suppose also that x is a real number that satisfies the equation

$$\frac{ax+b}{cx+d} = 1.$$

Must x be rational? If so, express x as a ratio of two integers.

* **29.** Suppose a, b, and c are integers and x, y, and z are nonzero real numbers that satisfy the following equations:

$$\frac{xy}{x+y} = a \quad \text{and} \quad \frac{xz}{x+z} = b \quad \text{and} \quad \frac{yz}{y+z} = c.$$

Is x rational? If so, express it as ratio of two integers.

30. Prove that if one solution for a quadratic equation of the form $x^2 + bx + c = 0$ is rational (where b and c are rational), then the other solution is also rational. (Use the fact that if the solutions of the equation are r and s, then $x^2 + bx + c = (x - r)(x - s)$.)

31. Prove that if a real number c satisfies a polynomial equation of the form

$$r_3x^3 + r_2x^2 + r_1x + r_0 = 0,$$

where r_0, r_1, r_2, and r_3 are rational numbers, then c satisfies an equation of the form

$$n_3x^3 + n_2x^2 + n_1x + n_0 = 0,$$

where n_0, n_1, n_2, and n_3 are integers.

Definition: A number c is called a **root** of a polynomial $p(x)$ if, and only if, $p(c) = 0$.

* **32.** Prove that for every real number c, if c is a root of a polynomial with rational coefficients, then c is a root of a polynomial with integer coefficients.

Use the properties of even and odd integers that are listed in Example 4.3.3 to do exercises 33 and 34.

33. When expressions of the form $(x - r)(x - s)$ are multiplied out, a quadratic polynomial is obtained. For instance, $(x - 2)(x - (-7)) = (x - 2)(x + 7) = x^2 + 5x - 14$.

***H* a.** What can be said about the coefficients of the polynomial obtained by multiplying out $(x - r)(x - s)$ when both r and s are odd integers? When both r and s are even integers? When one of r and s is even and the other is odd?

b. It follows from part (a) that $x^2 - 1253x + 255$ cannot be written as a product of two polynomials with integer coefficients. Explain why this is so.

* **34.** Observe that

$$(x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + (rs + rs + st)x - rst.$$

a. Derive a result for cubic polynomials similar to the result in part (a) of exercise 33 for quadratic polynomials.

b. Can $x^3 + 7x^2 - 8x - 27$ be written as a product of three polynomials with integer coefficients? Explain.

In 35–39 find the mistakes in the "proofs" that the sum of any two rational numbers is a rational number.

35. "**Proof:** Any two rational numbers produce a rational number when added together. So if r and s are particular but arbitrarily chosen rational numbers, then $r + s$ is rational."

36. "**Proof:** Let rational numbers $r = \frac{1}{4}$ and $s = \frac{1}{2}$ be given. Then $r + s = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$, which is a rational number. This is what was to be shown."

37. "**Proof:** Suppose r and s are rational numbers. By definition of rational, $r = a/b$ for some integers a and b with $b \neq 0$, and $s = a/b$ for some integers a and b with $b \neq 0$. Then

$$r + s = \frac{a}{b} + \frac{a}{b} = \frac{2a}{b}.$$

Let $p = 2a$. Then p is an integer since it is a product of integers. Hence $r + s = p/b$, where p and b are integers and $b \neq 0$. Thus $r + s$ is a rational number by definition of rational. This is what was to be shown."

38. "**Proof:** Suppose r and s are rational numbers. Then $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$ (by definition of rational). Then

$$r + s = \frac{a}{b} + \frac{c}{d}.$$

But this is a sum of two fractions, which is a fraction. So $r - s$ is a rational number since a rational number is a fraction."

39. "**Proof:** Suppose r and s are rational numbers. If $r + s$ is rational, then by definition of rational $r + s = a/b$ for some integers a and b with $b \neq 0$. Also since r and s are rational, $r = i/j$ and $s = m/n$ for some integers i, j, m, and n with $j \neq 0$ and $n \neq 0$. It follows that

$$r + s = \frac{i}{j} + \frac{m}{n} = \frac{a}{b},$$

which is a quotient of two integers with a nonzero denominator. Hence it is a rational number. This is what was to be shown."

ANSWERS FOR TEST YOURSELF

1. a ratio of integers with a nonzero denominator **2.** real number; not rational **3.** $0 = \frac{0}{1}$

4.4 Direct Proof and Counterexample IV: Divisibility

The essential quality of a proof is to compel belief. —Pierre de Fermat

When you were first introduced to the concept of division in elementary school, you were probably taught that 12 divided by 3 is 4 because if you separate 12 objects into groups of 3, you get 4 groups with nothing left over.

You may also have been taught to describe this fact by saying that "12 is evenly divisible by 3" or "3 divides 12 evenly."

The notion of divisibility is the central concept of one of the most beautiful subjects in advanced mathematics: **number theory**, the study of properties of integers.

Definition

If n and d are integers then

n is **divisible by** d if, and only if, n equals d times some integer and $d \neq 0$.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer, say } k, \text{ such that } n = dk \text{ and } d \neq 0.$$

The notation $\mathbf{d \nmid n}$ is read "d does not divide n."

Note According to the definition of divisibility if you know that n and d are any integers such that d divides n, then you may assume that d is not equal to zero.

Example 4.4.1 **Divisibility**

a. Is 21 divisible by 3?
b. Does 5 divide 40?
c. Does $7 \mid 42$?
d. Is 32 a multiple of -16?
e. Is 6 a factor of 54?
f. Is 7 a factor of -7?

Solution

a. Yes, $21 = 3 \cdot 7$.
b. Yes, $40 = 5 \cdot 8$.
c. Yes, $42 = 7 \cdot 6$.
d. Yes, $32 = (-16) \cdot (-2)$.
e. Yes, $54 = 6 \cdot 9$.
f. Yes, $-7 = 7 \cdot (-1)$. ■

Example 4.4.2 **Divisors of Zero**

If k is any nonzero integer, does k divide 0?

Solution Yes, because $0 = k \cdot 0$. ■

Two useful properties of divisibility are (1) that if one positive integer divides a second positive integer, then the first is less than or equal to the second, and (2) that the only divisors of 1 are 1 and -1.

Theorem 4.4.1 A Positive Divisor of a Positive Integer

For all integers a and b, if a and b are positive and a divides b then $a \leq b$.

Proof: Suppose a and b are any positive integers such that a divides b. *[We must show that $a \leq b$.]* By definition of divisibility, there exists an integer k so that $b = ak$. By property T25 of Appendix A, k must be positive because both a and b are positive. It follows that

$$1 \leq k$$

because every positive integer is greater than or equal to 1. Multiplying both sides by a gives

$$a \leq ka = b$$

because multiplying both sides of an inequality by a positive number preserves the inequality by property T20 of Appendix A. Thus $a \leq b$ *[as was to be shown].*

Theorem 4.4.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Proof: Since $1 \cdot 1 = 1$ and $(-1)(-1) = 1$, both 1 and -1 are divisors of 1. Now suppose m is any integer that divides 1. Then there exists an integer n such that $1 = mn$. By Theorem T25 in Appendix A, either both m and n are positive or both m and n are negative. If both m and n are positive, then m is a positive integer divisor of 1. By Theorem 4.4.1, $m \leq 1$, and, since the only positive integer that is less than or equal to 1 is 1 itself, it follows that $m = 1$. On the other hand, if both m and n are negative, then, by Theorem T12 in Appendix A, $(-m)(-n) = mn = 1$. In this case $-m$ is a positive integer divisor of 1, and so, by the same reasoning, $-m = 1$ and thus $m = -1$. Therefore there are only two possibilities: either $m = 1$ or $m = -1$. So the only divisors of 1 are 1 and -1.

Example 4.4.3 **Divisibility and Algebraic Expressions**

a. If a and b are integers, is $3a + 3b$ divisible by 3?

b. If k and m are integers, is $10km$ divisible by 5?

Solution

a. Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

b. Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers. ■

When the definition of divides is rewritten formally using the existential quantifier, the result is

$$d|n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk \text{ and } d \neq 0.$$

Note If $d = 0$, then $\frac{n}{d}$ is not defined, and so it is certainly not an integer.

Since the negation of an existential statement is universal, it follows that d does not divide n (denoted $d \nmid n$) if, and only if, $\forall$ integer k, $n \neq dk$ or $d = 0$; in other words, the quotient n/d is not an integer.

For all integers n and d, $\quad d \nmid n \quad \Leftrightarrow \quad \dfrac{n}{d}$ is not an integer.

Example 4.4.4 Checking Nondivisibility

Does $4|15$?

Solution No, $\frac{15}{4} = 3.75$, which is not an integer. ■

Caution! $a|b$ denotes the ***sentence*** "a divides b," whereas a/b denotes the ***number*** a divided by b.

Be careful to distinguish between the notation $a|b$ and the notation a/b. The notation $a|b$ stands for the sentence "a divides b," which means that there is an integer k such that $b = ak$. Dividing both sides by a gives $b/a = k$, an integer. Thus, when $a \neq 0$, $a|b$ if, and only if, b/a is an integer. On the other hand, the notation a/b stands for the number a/b which is the result of dividing a by b and which may or may not be an integer. In particular, since the symbol $|$ stands for the word "divides," be sure to avoid writing something like

$$\cancel{4|(3+5) = 4|8.}$$

If read out loud, this becomes "4 divides the quantity 3 plus 5 equals 4 divides 8," which is nonsense.

Example 4.4.5 Prime Numbers and Divisibility

An alternative way to define a prime number is to say that an integer $n > 1$ is prime if, and only if, its only positive integer divisors are 1 and itself. ■

Proving Properties of Divisibility

One of the most useful properties of divisibility is that it is transitive. If one number divides a second and the second number divides a third, then the first number divides the third.

Example 4.4.6 Transitivity of Divisibility

Prove that for all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.

Solution Since the statement to be proved is already written formally, you can immediately pick out the starting point, or first sentence of the proof, and the conclusion that must be shown.

Starting Point: Suppose a, b, and c are particular but arbitrarily chosen integers such that $a|b$ and $b|c$.

To Show: $a|c$.

You need to show that $a|c$, or, in other words, that

$$c = a \cdot (\text{some integer}).$$

But since $a|b$,

$$b = ar \quad \text{for some integer } r. \tag{4.4.1}$$

And since $b|c$,

$$c = bs \quad \text{for some integer } s. \tag{4.4.2}$$

Equation 4.4.2 expresses c in terms of b, and equation 4.4.1 expresses b in terms of a. Thus if you substitute 4.4.1 into 4.4.2, you will have an equation that expresses c in terms of a.

$$\begin{aligned} c &= bs && \text{by equation 4.4.2} \\ &= (ar)s && \text{by equation 4.4.1.} \end{aligned}$$

But $(ar)s = a(rs)$ by the associative law for multiplication. Hence

$$c = a(rs).$$

Now you are almost finished. You have expressed c as $a\cdot$(something). It remains only to verify that that something is an integer. But of course it is, because it is a product of two integers.

This discussion is summarized as follows:

Theorem 4.4.3 Transitivity of Divisibility

For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Proof: Suppose a, b, and c are any *[particular but arbitrarily chosen]* integers such that a divides b and b divides c. *[We must show that a divides c.]* By definition of divisibility,

$$b = ar \quad \text{and} \quad c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) && \text{by basic algebra.} \end{aligned}$$

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore

$$c = ak \quad \text{where } k \text{ is an integer.}$$

Thus a divides c by definition of divisibility. *[This is what was to be shown.]*

■

It would appear from the definition of prime that to show that an integer is prime you would need to show that it is not divisible by any integer greater than 1 and less than itself. In fact, you need only check whether it is divisible by a prime number less than or equal to itself. This follows from Theorems 4.4.1, 4.4.3, and the following theorem, which says that any integer greater than 1 is divisible by a prime number. The idea of the proof is quite simple. You start with a positive integer. If it is prime, you are done; if not, it is a product of two smaller positive factors. If one of these is prime, you are done; if not, you can pick one of the factors and write it as a product of still smaller positive factors. You can continue in this way, factoring the factors of the number you started with, until one of them turns out to

be prime. This must happen eventually because all the factors can be chosen to be positive and each is smaller than the preceding one.

Theorem 4.4.4 Divisibility by a Prime

Any integer $n > 1$ is divisible by a prime number.

Proof: Suppose n is a *[particular but arbitrarily chosen]* integer that is greater than 1. *[We must show that there is a prime number that divides n.]* If n is prime, then n is divisible by a prime number (namely itself), and we are done. If n is not prime, then, as discussed in Example 4.1.2b,

$$n = r_0 s_0 \quad \text{where } r_0 \text{ and } s_0 \text{ are integers and } 1 < r_0 < n \text{ and } 1 < s_0 < n.$$

It follows by definition of divisibility that $r_0 | n$.

If r_0 is prime, then r_0 is a prime number that divides n, and we are done. If r_0 is not prime, then

$$r_0 = r_1 s_1 \quad \text{where } r_1 \text{ and } s_1 \text{ are integers and } 1 < r_1 < r_0 \text{ and } 1 < s_1 < r_0.$$

It follows by the definition of divisibility that $r_1 | r_0$. But we already know that $r_0 | n$. Consequently, by transitivity of divisibility, $r_1 | n$.

If r_1 is prime, then r_1 is a prime number that divides n, and we are done. If r_1 is not prime, then

$$r_1 = r_2 s_2 \quad \text{where } r_2 \text{ and } s_2 \text{ are integers and } 1 < r_2 < r_1 \text{ and } 1 < s_2 < r_1.$$

It follows by definition of divisibility that $r_2 | r_1$. But we already know that $r_1 | n$. Consequently, by transitivity of divisibility, $r_2 | n$.

If r_2 is prime, then r_2 is a prime number that divides n, and we are done. If r_2 is not prime, then we may repeat the previous process by factoring r_2 as $r_3 s_3$.

We may continue in this way, factoring successive factors of n until we find a prime factor. We must succeed in a finite number of steps because each new factor is both less than the previous one (which is less than n) and greater than 1, and there are fewer than n integers strictly between 1 and n.* Thus we obtain a sequence

$$r_0, r_1, r_2, \ldots, r_k,$$

where $k \geq 0$, $1 < r_k < r_{k-1} < \cdots < r_2 < r_1 < r_0 < n$, and $r_i | n$ for each $i = 0, 1, 2, \ldots, k$. The condition for termination is that r_k should be prime. Hence r_k is a prime number that divides n. *[This is what we were to show.]*

Counterexamples and Divisibility

To show that a proposed divisibility property is not universally true, you need only find one pair of integers for which it is false.

*Strictly speaking, this statement is justified by an axiom for the integers called the well-ordering principle, which is discussed in Section 5.4. Theorem 4.4.4 can also be proved using strong mathematical induction, as shown in Example 5.4.1.

Example 4.4.7 **Checking a Proposed Divisibility Property**

Is the following statement true or false? For all integers a and b, if $a|b$ and $b|a$ then $a = b$.

Solution This statement is false. Can you think of a counterexample just by concentrating for a minute or so?

The following discussion describes a mental process that may take just a few seconds. It is helpful to be able to use it consciously, however, to solve more difficult problems.

To discover the truth or falsity of a statement such as the one given above, start off much as you would if you were trying to prove it.

Starting Point: Suppose a and b are integers such that $a|b$ and $b|a$.

Ask yourself, "*Must* it follow that $a = b$, or *could* it happen that $a \neq b$ for some a and b?" Focus on the supposition. What does it mean? By definition of divisibility, the conditions $a|b$ and $b|a$ mean that

$$b = ha \quad \text{and} \quad a = kb \quad \text{for some integers } h \text{ and } k.$$

Must it follow that $a = b$, or can you find integers a and b that satisfy these equations for which $a \neq b$? The equations imply that

$$b = ha = h(kb) = (hk)b.$$

Since $b|a$, $b \neq 0$, and so you can cancel b from the extreme left and right sides to obtain

$$1 = hk.$$

In other words, h and k are divisors of 1. But, by Theorem 4.4.2, the only divisors of 1 are 1 and -1. Thus h and k are both 1 or are both -1. If $h = k = 1$, then $b = a$. But if $h = k = -1$, then $b = -a$ and so $a \neq b$. This analysis suggests that you can find a counterexample by taking $b = -a$. Here is a formal answer:

Proposed Divisibility Property: For all integers a and b, if $a|b$ and $b|a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then $-2 = (-1)\cdot 2$ and $2 = (-1)\cdot(-2)$, and thus

$$a|b \text{ and } b|a, \text{ but } a \neq b \text{ because } 2 \neq -2.$$

Therefore, the statement is false.

■

The search for a proof will frequently help you discover a counterexample (provided the statement you are trying to prove is, in fact, false). Conversely, in trying to find a counterexample for a statement, you may come to realize the reason why it is true (if it is, in fact, true). The important thing is to keep an open mind until you are convinced by the evidence of your own careful reasoning.

The Unique Factorization of Integers Theorem

The most comprehensive statement about divisibility of integers is contained in the *unique factorization of integers theorem*. Because of its importance, this theorem is also called the

fundamental theorem of arithmetic. Although Euclid, who lived about 300 B.C.E., seems to have been acquainted with the theorem, it was first stated precisely by the great German mathematician Carl Friedrich Gauss (rhymes with *house*) in 1801.

The unique factorization of integers theorem says that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order in which the primes are written. For example,

$$72 = 2\cdot2\cdot2\cdot3\cdot3 = 2\cdot3\cdot3\cdot2\cdot2 = 3\cdot2\cdot2\cdot3\cdot2,$$

and so forth. The three 2's and two 3's may be written in any order, but any factorization of 72 as a product of primes must contain exactly three 2's and two 3's—no other collection of prime numbers besides three 2's and two 3's multiplies out to 72.

Note This theorem is the reason the number 1 is not allowed to be prime. If 1 were prime, then factorizations would not be unique. For example, $6 = 2\cdot3 = 1\cdot2\cdot3$, and so forth.

Theorem 4.4.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

The proof of the unique factorization of integers theorem is outlined in the exercises for Sections 5.4 and 8.4.

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right.

Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer, $p_1, p_2, \ldots, p_k$ are prime numbers, $e_1, e_2, \ldots, e_k$ are positive integers, and $p_1 < p_2 < \cdots < p_k$.

Example 4.4.8 **Writing Integers in Standard Factored Form**

Write 3,300 in standard factored form.

Solution First find all the factors of 3,300. Then write them in ascending order:

$$\begin{aligned} 3{,}300 &= 100\cdot33 = 4\cdot25\cdot3\cdot11 \\ &= 2\cdot2\cdot5\cdot5\cdot3\cdot11 = 2^2\cdot3^1\cdot5^2\cdot11^1. \end{aligned}$$

■

Example 4.4.9 **Using Unique Factorization to Solve a Problem**

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

Does $17 \mid m$?

Solution Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem). But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large). Hence 17 must occur as one of the prime factors of m, and so $17 \mid m$. ■

TEST YOURSELF

1. To show that a nonzero integer d divides an integer n, we must show that _____.
2. To say that d divides n means the same as saying that _____ is divisible by _____.
3. If a and b are positive integers and $a \mid b$, then _____ is less than or equal to _____.
4. For all integers n and d, $d \nmid n$ if, and only if, _____.
5. If a and b are integers, the notation $a \mid b$ denotes _____ and the notation a/b denotes _____.
6. The transitivity of divisibility theorem says that for all integers a, b, and c, if _____ then _____.
7. The divisibility by a prime theorem says that every integer greater than 1 is _____.
8. The unique factorization of integers theorem says that any integer greater than 1 is either _____ or can be written as _____ in a way that is unique except possibly for the _____ in which the numbers are written.

EXERCISE SET 4.4

Give a reason for your answer in each of 1–13. Assume that all variables represent integers.

1. Is 52 divisible by 13?
2. Does $7 \mid 56$?
3. Does $5 \mid 0$?
4. Does 3 divide $(3k+1)(3k+2)(3k+3)$?
5. Is $6m(2m+10)$ divisible by 4?
6. Is 29 a multiple of 3?
7. Is -3 a factor of 66?
8. Is $6a(a+b)$ a multiple of $3a$?
9. Is 4 a factor of $2a \cdot 34b$?
10. Does $7 \mid 34$?
11. Does $13 \mid 73$?
12. If $n = 4k+1$, does 8 divide $n^2 - 1$?
13. If $n = 4k+3$, does 8 divide $n^2 - 1$?
14. Fill in the blanks in the following proof that for all integers a and b, if $a \mid b$ then $a \mid (-b)$.

    Proof: Suppose a and b are any integers such that __(a)__. By definition of divisibility, there exists an integer r such that __(b)__. By substitution,

    $$-b = -(ar) = a(-r).$$

    Let $t =$ __(c)__. Then t is an integer because $t = (-1) \cdot r$, and both -1 and r are integers. Thus, by substitution, $-b = at$, where t is an integer, and so by definition of divisibility, __(d)__, as was to be shown.

Prove statements 15 and 16 directly from the definition of divisibility.

15. For all integers a, b, and c, if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$.

H 16. For all integers a, b, and c, if $a \mid b$ then $a \mid c$ then $a \mid (b-c)$.

17. For all integers a, b, c, and d, if $a \mid c$ and $b \mid d$ then $ab \mid cd$.

18. Consider the following statement: The negative of any multiple of 3 is a multiple of 3.
- **a.** Write the statement formally using a quantifier and a variable.
- **b.** Determine whether the statement is true or false and justify your answer.

19. Show that the following statement is false: For all integers a and b, if $3|(a+b)$ then $3|(a-b)$.

For each statement in 20–32, determine whether the statement is true or false. Prove the statement directly from the definitions if it is true, and give a counterexample if it is false.

***H* 20.** The sum of any three consecutive integers is divisible by 3.

21. The product of any two even integers is a multiple of 4.

***H* 22.** A necessary condition for an integer to be divisible by 6 is that it be divisible by 2.

23. A sufficient condition for an integer to be divisible by 8 is that it be divisible by 16.

24. For all integers a, b, and c, if $a|b$ and $a|c$ then $a|(2b-3c)$.

25. For all integers a, b, and c, if a is a factor of c and b is a factor of c then ab is a factor of c.

***H* 26.** For all integers a, b, and c, if $ab|c$ then $a|c$ and $b|c$.

***H* 27.** For all integers a, b, and c, if $a|(b+c)$ then $a|b$ or $a|c$.

28. For all integers a, b, and c, if $a|bc$ then $a|b$ or $a|c$.

29. For all integers a and b, if $a|b$ then $a^2|b^2$.

30. For all integers a and n, if $a|n^2$ and $a \leq n$ then $a|n$.

31. For all integers a and b, if $a|10b$ then $a|10$ or $a|b$.

32. A fast-food chain has a contest in which a card with numbers on it is given to each customer who makes a purchase. If some of the numbers on the card add up to 100, then the customer wins \$100. A certain customer receives a card containing the numbers

72, 21, 15, 36, 69, 81, 9, 27, 42, and 63.

Will the customer win \$100? Why or why not?

33. Is it possible to have a combination of nickels, dimes, and quarters that add up to \$4.72? Explain.

34. Consider a string consisting of a's, b's, and c's where the number of b's is three times the number of a's and the number of c's is five times the number of a's. Prove that the length of the string is divisible by 3.

35. Two athletes run a circular track at a steady pace so that the first completes one round in 8 minutes and the second in 10 minutes. If they both start from the same spot at 4 P.M., when will be the first time they return to the start together?

36. It can be shown (see exercises 44–48) that an integer is divisible by 3 if, and only if, the sum of its digits is divisible by 3; an integer is divisible by 9 if, and only if, the sum of its digits is divisible by 9; an integer is divisible by 5 if, and only if, its right-most digit is a 5 or a 0; and an integer is divisible by 4 if, and only if, the number formed by its right-most two digits is divisible by 4. Check the following integers for divisibility by 3, 4, 5, and 9.
- **a.** 637,425,403,705,125
- **b.** 12,858,306,120,312
- **c.** 517,924,440,926,512
- **d.** 14,328,083,360,232

37. Use the unique factorization theorem to write the following integers in standard factored form.
a. 1,176 **b.** 5,733 **c.** 3,675

38. Let $n = 8{,}424$.
- **a.** Write the prime factorization for n.
- **b.** Write the prime factorization for n^5.
- ***H* c.** Is n^5 divisible by 20? Explain.
- ***H* d.** What is the least positive integer m so that $8{,}424 \cdot m$ is a perfect square?

39. Suppose that in standard factored form $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where k is a positive integer; p_1, $p_2, \dots, p_k$ are prime numbers; and $e_1, e_2, \dots, e_k$ are positive integers.
- **a.** What is the standard factored form for a^3?
- **b.** Find the least positive integer k such that $2^4 \cdot 3^5 \cdot 7 \cdot 11^2 \cdot k$ is a perfect cube (that is, it equals an integer to the third power). Write the resulting product as a perfect cube.

40. a. If a and b are integers and $12a = 25b$, does $12|b$? does $25|a$? Explain.
- **b.** If x and y are integers and $10x = 9y$, does $10|y$? does $9|x$? Explain.

H 41. How many zeros are at the end of $45^8 \cdot 88^5$? Explain how you can answer this question without actually computing the number. (*Hint:* $10 = 2 \cdot 5$.)

42. If n is an integer and $n > 1$, then $n!$ is the product of n and every other positive integer that is less than n. For example, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

a. Write 6! in standard factored form.

b. Write 20! in standard factored form.

c. Without computing the value of $(20!)^2$ determine how many zeros are at the end of this number when it is written in decimal form. Justify your answer.

H* 43. At a certain university $2/3$ of the mathematics students and $3/5$ of the computer science students have taken a discrete mathematics course. The number of mathematics students who have taken the course equals the number of computer science students who have taken the course. If there are at least 100 mathematics students at the university, what are the least possible number of mathematics students and the least possible number of computer science students at the university?

Definition: Given any nonnegative integer n, the **decimal representation** of n is an expression of the form

$$d_k\, d_{k-1} \cdots d_2 d_1 d_0,$$

where k is a nonnegative integer, $d_0, d_1, d_2, \ldots, d_k$ (called the **decimal digits** of n) are integers from 0 to 9 inclusive, $dk \neq 0$ unless $n = 0$ and $k = 0$, and

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0.$$

(For example, $2{,}503 = 2 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10 + 3$.)

44. Prove that if n is any nonnegative integer whose decimal representation ends in 0, then $5 \mid n$. (*Hint:* If the decimal representation of a nonnegative integer n ends in d_0, then $n = 10m + d_0$ for some integer m.)

45. Prove that if n is any nonnegative integer whose decimal representation ends in 5, then $5 \mid n$.

46. Prove that if the decimal representation of a nonnegative integer n ends in $d_1 d_0$ and if $4 \mid (10d_1 + d_0)$, then $4 \mid n$. (*Hint:* If the decimal representation of a nonnegative integer n ends in $d_1 d_0$, then there is an integer s such that $n = 100s + 10d_1 + d_0$.)

H* 47. Observe that

$$\begin{aligned} 7{,}524 &= 7 \cdot 1{,}000 + 5 \cdot 100 + 2 \cdot 10 + 4 \\ &= 7(999 + 1) + 5(99 + 1) + 2(9 + 1) + 4 \\ &= (7 \cdot 999 + 7) + (5 \cdot 99 + 5) + (2 \cdot 9 + 2) + 4 \\ &= (7 \cdot 999 + 5 \cdot 99 + 2 \cdot 9) + (7 + 5 + 2 + 4) \\ &= (7 \cdot 111 \cdot 9 + 5 \cdot 11 \cdot 9 + 2 \cdot 9) + (7 + 5 + 2 + 4) \\ &= (7 \cdot 111 + 5 \cdot 11 + 2) \cdot 9 + (7 + 5 + 2 + 4) \\ &= (\text{an integer divisible by 9}) \\ &\qquad + (\text{the sum of the digits of 7,524}). \end{aligned}$$

Since the sum of the digits of 7,524 is divisible by 9, 7,524 can be written as a sum of two integers each of which is divisible by 9. It follows from exercise 15 that 7,524 is divisible by 9.

Generalize the argument given in this example to any nonnegative integer n. In other words, prove that for any nonnegative integer n, if the sum of the digits of n is divisible by 9, then n is divisible by 9.

*** 48.** Prove that for any nonnegative integer n, if the sum of the digits of n is divisible by 3, then n is divisible by 3.

*** 49.** Given a positive integer n written in decimal form, the alternating sum of the digits of n is obtained by starting with the right-most digit, subtracting the digit immediately to its left, adding the next digit to the left, subtracting the next digit, and so forth. For example, the alternating sum of the digits of 180,928 is $8 - 2 + 9 - 0 + 8 - 1 = 22$. Justify the fact that for any nonnegative integer n, if the alternating sum of the digits of n is divisible by 11, then n is divisible by 11.

50. The integer 123,123 has the form abc,abc, where a, b, and c are integers from 0 through 9. Consider all six-digit integers of this form. Which prime numbers divide every one of these integers? Prove your answer.

ANSWERS FOR TEST YOURSELF

1. n equals d times some integer and $d \neq 0$ (*Or:* there is an integer r such that $n = dr$ and $d \neq 0$) **2.** n; d **3.** a; b **4.** $\frac{n}{d}$ is not an integer **5.** the sentence "a divides b"; the number obtained when a is divided by b **6.** a divides b and b divides c; a divides c **7.** divisible by some prime number **8.** prime; a product of prime numbers; order

4.5 Direct Proof and Counterexample V: Division into Cases and the Quotient-Remainder Theorem

Be especially critical of any statement following the word "obviously."
—Anna Pell Wheeler, 1883–1966

When you divide 11 by 4, you get a quotient of 2 and a remainder of 3.

$$\begin{array}{r} 2 \leftarrow \text{quotient} \\ 4\overline{)11} \\ \underline{8} \\ 3 \leftarrow \text{remainder} \end{array}$$

Another way to say this is that 11 equals 2 groups of 4 with 3 left over:

$$\boxed{xxx}\ \boxed{xxx}\ xxx$$

2 groups of 4 — 3 left over

Or,

$$11 = 2 \cdot 4 + 3.$$

2 groups of 4 — 3 left over

The number left over (3) is less than the size of the groups (4) because if 4 or more were left over, another group of 4 could be formed.

The quotient-remainder theorem says that when any integer n is divided by any positive integer d, the result is a quotient q and a nonnegative integer remainder r that is smaller than d.

Theorem 4.5.1 The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

The proof that there exist integers q and r with the given properties is in Section 5.4; the proof that q and r are unique is outlined in exercise 21 in Section 4.8.

If n is positive, the quotient-remainder theorem can be illustrated on the number line as follows:

If n is negative, the picture changes. Since $n = dq + r$, where r is nonnegative, d must be multiplied by a negative integer q to bring dq either exactly to n (in which case $r = 0$) or to a point below n (in which case the positive integer r is added to bring $dq + r$ back up to n). This is illustrated as follows:

Example 4.5.1 **The Quotient-Remainder Theorem**

For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

a. $n = 54, d = 4$ b. $n = -54, d = 4$ c. $n = 54, d = 70$

Solution

a. $54 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$.

b. $-54 = 4 \cdot (-14) + 2$; hence $q = -14$ and $r = 2$.

c. $54 = 70 \cdot 0 + 54$; hence $q = 0$ and $r = 54$. ■

div and *mod*

A number of computer languages have built-in functions that enable you to compute values of the quotients and remainders for the quotient-remainder theorem. In Python *n div d* is written *n* // *d* and *n mod d* is written *n* % *d*, and for all integer inputs both operators give the values that satisfy the quotient-remainder theorem. In C, C#, and Java, *n div d* is written *n* / *d* and *n mod d* is written *n* % *d*. For all nonnegative integer inputs for *n* and positive integer inputs for *d*, both operators give the values that satisfy the quotient-remainder theorem, but for negative integer inputs for *n* or *d* the resulting values differ from their mathematical counterparts.

Definition

Given an integer n and a positive integer d,

$$\textbf{\textit{n div d}} = \text{the integer quotient obtained when } n \text{ is divided by } d, \text{ and}$$

$$\textbf{\textit{n mod d}} = \text{the nonnegative integer remainder obtained when } n \text{ is divided by } d.$$

Symbolically, if n and d are integers and $d > 0$, then

$$n \; div \; d = q \quad \text{and} \quad n \; mod \; d = r \quad \Leftrightarrow \quad n = dq + r,$$

where q and r are integers and $0 \leq r < d$.

Note In 1801 Carl Friedrich Gauss introduced the word *modulus* and its abbreviation *mod* with the meaning shown here.

It follows from the quotient-remainder theorem that $n \; mod \; d$ equals one of the integers from 0 through $d - 1$ (since the remainder of the division of n by d must be one of these integers). Also a necessary and sufficient condition for an integer n to be divisible by an integer d is that $n \; mod \; d = 0$. You are asked to prove this in the exercises at the end of this section.

Example 4.5.2 **Computing *div* and *mod* by Hand or with a Four-Function Calculator**

Compute 32 *div* 9 and 32 *mod* 9 by hand or with a four-function calculator.

Solution Performing the division by hand gives the following results:

$$\begin{array}{r} 3 \quad \longleftarrow 32 \; div \; 9 \\ 9\overline{)32} \\ \underline{27} \\ 5 \quad \longleftarrow 32 \; mod \; 9 \end{array}$$

To use a four-function calculator to compute $n \; div \; d$ for a nonnegative integer n and a positive integer d, just divide n by d and ignore the part of the answer to the right of the decimal point. To compute $n \; mod \; d$, substitute $n \; div \; d$ in place of q and $n \; mod \; d$ in place of r in the equation $n = dq + r$. The result is

$$n = d \cdot (n \; div \; d) + n \; mod \; d.$$

Solving for $n \; mod \; d$ gives

$$n \; mod \; d = n - d \cdot (n \; div \; d).$$

Thus when you use a four-function calculator to divide 32 by 9, you obtain an expression like 3.555555556. Discarding the fractional part gives $32 \; div \; 9 = 3$, and so

$$32 \; mod \; 9 = 32 - 9 \cdot (32 \; div \; 9) = 32 - 27 = 5. \quad \blacksquare$$

Example 4.5.3 **Computing the Day of the Week**

Suppose today is Tuesday, and neither this year nor next year is a leap year. What day of the week will it be 1 year from today?

Solution There are 365 days in a year that is not a leap year, and each week has 7 days. Now

$$365 \; div \; 7 = 52 \quad \text{and} \quad 365 \; mod \; 7 = 1$$

because $365 = 52 \cdot 7 + 1$. Thus 52 weeks, or 364 days, from today will be a Tuesday, and so 365 days from today will be 1 day later, namely, Wednesday.

More generally, if *DayT* is the day of the week today and *DayN* is the day of the week in N days, then

$$DayN = (DayT + N) \; mod \; 7, \tag{4.5.1}$$

where Sunday $= 0$, Monday $= 1, \ldots,$ Saturday $= 6$. $\blacksquare$

Example 4.5.4 **Solving Problems about *mod***

a. Prove that if n is a positive integer, then $n \; mod \; 10$ is the digit in the ones place in the decimal representation for n. (See Section 2.5 or the preamble to exercises 44–49 in Section 4.4 for discussion about the decimal representation of integers.)

b. Suppose m is an integer. If $m \; mod \; 11 = 6$, what is $4m \; mod \; 11$?

Solution

a. **Proof:** Suppose n is any positive integer. The decimal representation for n is $d_k d_{k-1} \ldots d_2 d_1 d_0$, where $d_0, d_1, d_2, \ldots, d_k$ are integers from 0 to 9 inclusive, $d_k \neq 0$ unless $n = 0$ and $k = 0$,

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0,$$

and d_0 is the digit in the ones place. Factoring out 10 from all but the final term gives

$$n = 10 \cdot (d_k \cdot 10^{k-1} + d_{k-1} \cdot 10^{k-2} + \cdots + d_2 \cdot 10^1 + d_1) + d_0.$$

Thus $n = 10 \cdot (\text{an integer}) + d_0$, and so $n \; mod \; 10 = d_0$, which is the digit in the ones place in the decimal representation for n.

b. Because $m \; mod \; 11 = 6$, the remainder obtained when m is divided by 11 is 6. This means that there is some integer q so that

$$m = 11q + 6.$$

Thus $$4m = 44q + 24 = 44q + 22 + 2 = 11(4q + 2) + 2.$$

Since $4q + 2$ is an integer (because products and sums of integers are integers) and since $2 < 11$, the remainder obtained when $4m$ is divided by 11 is 2. Therefore,

$$4m \; mod \; 11 = 2.$$ ■

Representations of Integers

In Section 4.1 we defined an even integer to have the form twice some integer. At that time we could have defined an odd integer to be one that was not even. Instead, because it was more useful for proving theorems, we specified that an odd integer has the form twice some integer plus 1. The quotient-remainder theorem brings these two ways of describing odd integers together by guaranteeing that any integer is either even or odd. To see why, let n be any integer, and consider what happens when n is divided by 2. By the quotient-remainder theorem (with $d = 2$), there exist unique integers q and r such that

$$n = 2q + r \quad \text{and} \quad 0 \le r < 2.$$

But the only integers that satisfy $0 \le r < 2$ are $r = 0$ and $r = 1$. It follows that given any integer n, there exists an integer q with

$$n = 2q + 0 \quad \text{or} \quad n = 2q + 1.$$

In the case that $n = 2q + 0 = 2q$, n is even. In the case that $n = 2q + 1$, n is odd. Hence n is either even or odd, and, because of the uniqueness of q and r, n cannot be both even and odd.

Note The fact that any integer is either even or odd is called the **parity property**.

The ***parity*** of an integer refers to whether the integer is even or odd. For instance, 5 has odd parity and 28 has even parity.

Example 4.5.5 **Consecutive Integers Have Opposite Parity**

Prove that given any two consecutive integers, one is even and the other is odd.

Solution Two integers are called *consecutive* if, and only if, one is one more than the other. So if one integer is m, the next consecutive integer is $m + 1$.

To prove the given statement, you can divide the analysis into two cases: case 1, where the smaller of the two integers is even, and case 2, where the smaller of the two integers is odd.

Theorem 4.5.2 The Parity Property

Any two consecutive integers have opposite parity.

Proof:

Suppose that two *[particular but arbitrarily chosen]* consecutive integers are given; call them m and $m + 1$. *[We must show that one of m and $m + 1$ is even and that the other is odd.]* By the parity property, either m is even or m is odd. *[We break the proof into two cases depending on whether m is even or odd.]*

Case 1 (m is even): In this case, $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd *[by definition of odd]*. Hence in this case, one of m and $m + 1$ is even and the other is odd.

(continued on page 204)

Case 2 (m is odd): In this case, $m = 2k + 1$ for some integer k, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer, and thus $m + 1$ is even. Hence in this case also, one of m and $m + 1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular m and $m + 1$ that are chosen, one of m and $m + 1$ is even and the other is odd. *[This is what was to be shown.]*

■

The division into cases in a proof is like the transfer of control for an **if-then-else** statement in a computer program. If m is even, control transfers to case 1; if not, control transfers to case 2. For any given integer, only one of the cases will apply. You must consider both cases, however, to obtain a proof that is valid for an arbitrarily given integer whether even or not.

There are times when division into more than two cases is called for. Suppose that at some stage of developing a proof, you know that a statement of the form

$$A_1 \text{ or } A_2 \text{ or } A_3 \text{ or } \ldots \text{ or } A_n$$

is true, and suppose you want to deduce a conclusion C. By definition of *or*, you know that at least one of the statements A_i is true (although you may not know which). In this situation, you should use the method of division into cases. First assume A_1 is true and deduce C; next assume A_2 is true and deduce C; and so forth, until you have assumed A_n is true and deduced C. At that point, you can conclude that regardless of which statement A_i happens to be true, the truth of C follows.

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or . . . or A_n, then C," prove all of the following:

If A_1, then C,
If A_2, then C,
⋮
If A_n, then C.

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Proof by division into cases is a generalization of the argument form shown in Example 2.3.7, whose validity you were asked to establish in exercise 21 of Section 2.3. This method of proof was combined with the quotient-remainder theorem for $d = 2$ to prove Theorem 4.5.2. Allowing d to take on additional values makes it possible to obtain a variety of other results. We begin by showing what happens when $a = 4$.

Example 4.5.6 **Representing Integers *mod* 4**

Show that any integer can be written in one of the four forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q.

Solution Given any integer n, apply the quotient-remainder theorem to n with the divisor equal to 4. This implies that there exist an integer quotient q and a remainder r such that

$$n = 4q + r \quad \text{and} \quad 0 \le r < 4.$$

But the only nonnegative remainders r that are less than 4 are 0, 1, 2, and 3. Hence

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q. In other words, n *mod* 4 equals 0, 1, 2, or 3. ■

The next example illustrates how the alternative representations for integers *mod* 4 can help establish a result in number theory. The solution is broken into two parts: a discussion and a formal proof. These correspond to the stages of actual proof development. Very few people, when asked to prove an unfamiliar theorem, immediately write down the kind of formal proof you find in a mathematics text. They may first check some examples to explore whether the theorem is believable. If it passes that test, they often need to experiment with several possible approaches before finding one that works. A formal proof is much like the ending of a mystery story—the part in which the action of the story is systematically reviewed and all the loose ends are carefully tied together.

Example 4.5.7 **The Square of an Odd Integer**

Prove: The square of any odd integer has the form $8m + 1$ for some integer m.

Note Another way to state this fact is that if you square an odd integer and divide by 8, you will always get a remainder of 1. Try a few examples!

Solution If checking some examples convinces you that the statement may be true, begin to develop a proof by asking, "Where am I starting from?" and "What do I need to show?" To help answer these questions, introduce variables to rewrite the statement more formally.

Formal Restatement: $\forall$ odd integer n, $\exists$ an integer m such that $n^2 = 8m + 1$.

From this, you can immediately identify the starting point and what is to be shown.

Starting Point: Suppose n is a particular but arbitrarily chosen odd integer.

To Show: $\exists$ an integer m such that $n^2 = 8m + 1$.

This looks tough. Why should there be an integer m with the property that $n^2 = 8m + 1$? That would say that $(n^2 - 1)/8$ is an integer, or that 8 divides $n^2 - 1$. Perhaps you could make use of the fact that $n^2 - 1 = (n - 1)(n + 1)$. Does 8 divide $(n - 1)(n + 1)$? Since n is odd, both $(n - 1)$ and $(n + 1)$ are even. That means that their product is divisible by 4. But that's not enough. You need to show that the product is divisible by 8.

Note Desperation can spur creativity. When you have tried all the obvious approaches without success and you really care about solving a problem, you reach into the odd corners of your memory for *anything* that may help.

You could try another approach by arguing that since n is odd, you can represent it as $2q + 1$ for some integer q. Then $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$. It is clear from this analysis that n^2 can be written in the form $4m$+1, but it may not be clear that it can be written as $8m + 1$.*

Yet another possibility is to use the result of Example 4.5.6. That example showed that any integer can be written in one of the four forms $4q$, $4q + 1$, $4q + 2$, or $4q + 3$. Two of these, $4q + 1$ and $4q + 3$, are odd. Thus any odd integer can be written in the form $4q + 1$ or $4q + 3$ for some integer q. You could try breaking into cases based on these two different forms.

*See exercise 18 for a different perspective about this approach.

It turns out that this last possibility works! In each of the two cases, the conclusion follows readily by direct calculation. The details are shown in the following formal proof:

Theorem 4.5.3

The square of any odd integer has the form $8m + 1$ for some integer m.

Proof: Suppose n is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem with the divisor equal to 4, n can be written in one of the forms

$$4q \quad \text{or} \quad 4q + 1 \quad \text{or} \quad 4q + 2 \quad \text{or} \quad 4q + 3$$

for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms

$$4q + 1 \quad \text{or} \quad 4q + 3.$$

Case 1 ($n = 4q + 1$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q + 1)^2 && \text{by substitution} \\ &= (4q + 1)(4q + 1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Case 2 ($n = 4q + 3$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{by substitution} \\ &= (4q + 3)(4q + 3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8 + 1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

[The motivation for the choice of algebra steps was the desire to write the expression in the form $8 \cdot$(some integer) $+ 1$.]

Let $m = 2q^2 + 3q + 1$. Then m is an integer since 1, 2, 3, and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. *[This is what we needed to show.]*

Note that the result of Theorem 4.5.3 can also be written, "For any odd integer n, n^2 *mod* $8 = 1$."

In general, according to the quotient-remainder theorem, if an integer n is divided by an integer d, the possible remainders are $0, 1, 2, \ldots, (d-1)$. This implies that n can be written in one of the forms

$$dq,\ dq+1,\ dq+2,\ \ldots,\ dq+(d-1) \quad \text{for some integer } q.$$

Many properties of integers can be obtained by giving d a variety of different values and analyzing the cases that result.

Absolute Value and the Triangle Inequality

The triangle inequality is one of the most important results involving absolute value. It has applications in many areas of mathematics.

Definition

For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

The triangle inequality says that the absolute value of the sum of two numbers is less than or equal to the sum of their absolute values. We give a proof based on the following two facts, both of which are derived using division into cases. We state both as lemmas. A **lemma** is a statement that does not have much intrinsic interest but is helpful in deriving other results.

Lemma 4.5.4

For every real number r, $-|r| \leq r \leq |r|$.

Proof: Suppose r is any real number. We divide into cases according to whether $r = 0$, $r > 0$, or $r < 0$.

Case 1 ($r = 0$): In this case, by definition of absolute value, $|r| = r = 0$. since $0 = -0$, we have that $-0 = -|r| = 0 = r = |r|$, and so it is true that

$$-|r| \leq r \leq |r|.$$

Case 2 ($r > 0$): In this case, by definition of absolute value, [&|pipe|r|pipe||=|r&]. Also, since r is positive and $-|r|$ is negative, $-|r| < r$. Thus it is true that

$$-|r| \leq r \leq |r|.$$

Case 3 ($r < 0$): In this case, by definition of absolute value, $|r| = -r$. Multiplying both sides by -1 gives that $-|r| = r$. Also, since r is negative and $|r|$ is positive, $r < |r|$. Thus it is also true in this case that

$$-|r| \leq r \leq |r|.$$

Hence, in every case,

$$-|r| \leq r \leq |r|$$

[as was to be shown].

Lemma 4.5.5

For every real number r, $|-r| = |r|$.

Proof: Suppose r is any real number. By Theorem T23 in Appendix A, if $r > 0$, then $-r < 0$, and if $r < 0$, then $-r > 0$. Thus

$$|-r| = \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ -(-r) & \text{if } -r < 0 \end{cases} \quad \text{by definition of absolute value}$$

$$= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } r = 0 \\ r & \text{if } -r < 0 \end{cases} \quad \text{because } -(-r) = r \text{ by Theorem T4 in Appendix A, and when } -r = 0, \text{ then } r = 0$$

$$= \begin{cases} -r & \text{if } r < 0 \\ 0 & \text{if } r = 0 \\ r & \text{if } r > 0 \end{cases} \quad \text{because, by Theorem T24 in Appendix A, when } -r > 0, \text{ then } r < 0, \text{ when } -r < 0, \text{ then } r > 0$$

$$= \begin{cases} r & \text{if } r \geq 0 \\ -r & \text{if } r < 0 \end{cases} \quad \text{by reformatting the previous result}$$

$$= |r| \quad \text{by definition of absolute value.}$$

Lemmas 4.5.4 and 4.5.5 now provide a basis for proving the triangle inequality.

Theorem 4.5.6 The Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

Proof: Suppose x and y are any real numbers.

Case 1 ($x + y \geq 0$): In this case, $|x + y| = x + y$, and so, by Lemma 4.5.4,

$$x \leq |x| \quad \text{and} \quad y \leq |y|.$$

Hence, by Theorem T26 of Appendix A,

$$|x + y| = x + y \leq |x| + |y|.$$

Case 2 ($x + y < 0$): In this case, $|x + y| = -(x + y) = (-x) + (-y)$, and so, by Lemmas 4.5.4 and 4.5.5,

$$-x \leq |-x| = |x| \quad \text{and} \quad -y \leq |-y| = |y|.$$

It follows, by Theorem T26 of Appendix A, that

$$|x + y| = (-x) + (-y) \leq |x| + |y|.$$

Hence in both cases $|x + y| \leq |x| + |y|$ *[as was to be shown].*

TEST YOURSELF

1. The quotient-remainder theorem says that for all integers n and d with $d \geq 0$, there exist _____ q and r such that _____ and _____.
2. If n and d are integers with $d > 0$, n *div* d is _____ and n *mod* d is _____.
3. The parity of an integer indicates whether the integer is _____.
4. According to the quotient-remainder theorem, if an integer n is divided by a positive integer d, the possible remainders are _____. This implies that n can be written in one of the forms _____ for some integer q.
5. To prove a statement of the form "If A_1 or A_2 or A_3, then C," prove _____ and _____ and _____.
6. The triangle inequality says that for all real numbers x and y, _____.

EXERCISE SET 4.5

For each of the values of n and d given in 1–6, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

1. $n = 70, d = 9$
2. $n = 62, d = 7$
3. $n = 36, d = 40$
4. $n = 3, d = 11$
5. $n = -45, d = 11$
6. $n = -27, d = 8$

Evaluate the expressions in 7–10.

7. **a.** 43 *div* 9 **b.** 43 *mod* 9
8. **a.** 50 *div* 7 **b.** 50 *mod* 7
9. **a.** 28 *div* 5 **b.** 28 *mod* 5
10. **a.** 30 *div* 2 **b.** 30 *mod* 2
11. Check the correctness of formula (4.5.1) given in Example 4.5.3 for the following values of *DayT* and *N*.
    a. *DayT* = 6 (Saturday) and $N = 15$
    b. *DayT* = 0 (Sunday) and $N = 7$
    c. *DayT* = 4 (Thursday) and $N = 12$

* 12. Justify formula (4.5.1) for general values of *DayT* and *N*.

13. On a Monday a friend says he will meet you again in 30 days. What day of the week will that be?

H 14. If today is Tuesday, what day of the week will it be 1,000 days from today?

15. January 1, 2000, was a Saturday, and 2000 was a leap year. What day of the week will January 1, 2050, be?

16. Suppose d is a positive and n is any integer. If $d|n$, what is the remainder obtained when the quotient-remainder theorem is applied to n with divisor d?

17. Prove directly from the definitions that for every integer n, $n^2 - n + 3$ is odd. Use division into two cases: n is even and n is odd.

18. **a.** Prove that the product of any two consecutive integers is even.
    b. The result of part (a) suggests that the second approach in the discussion of Example 4.5.7 might be possible after all. Write a new proof of Theorem 4.5.3 based on this observation.

19. Prove directly from the definitions that for all integers m and n, if m and n have the same parity, then $5m + 7n$ is even. Divide into two cases: m and n are both even and m and n are both odd.

20. Suppose a is any integer. If a *mod* 7 = 4, what is 5a *mod* 7? In other words, if division of a by 7 gives a remainder of 4, what is the remainder when 5a is divided by 7? Your solution should show that you obtain the same answer no matter what integer you start with.

21. Suppose b is any integer. If b *mod* 12 = 5, what is 8b *mod* 12? In other words, if division of b by 12 gives a remainder of 5, what is the remainder when 8b is divided by 12? Your solution should show that you obtain the same answer no matter what integer you start with.

22. Suppose c is any integer. If c *mod* 15 = 3, what is 10c *mod* 15? In other words, if division of c by 15 gives a remainder of 3, what is the remainder when 10c is divided by 15? Your solution should show that you obtain the same answer no matter what integer you start with.

23. Prove that for every integer n, if n mod 5 = 3 then $n^2 \ mod \ 5 = 4$.

24. Prove that for all integers m and n, if $m \ mod \ 5 = 2$ and $n \ mod \ 5 = 1$ then $mn \ mod \ 5 = 2$.

25. Prove that for all integers a and b, if $a \ mod \ 7 = 5$ and $b \ mod \ 7 = 6$ then $ab \ mod \ 7 = 2$.

H 26. Prove that a necessary and sufficient condition for an integer n to be divisible by a positive integer d is that $n \ mod \ d = 0$.

H 27. Use the quotient-remainder theorem with divisor equal to 2 to prove that the square of any integer can be written in one of the two forms $4k$ or $4k + 1$ for some integer k.

H 28. **a.** Prove: Given any set of three consecutive integers, one of the integers is a multiple of 3.
b. Use the result of part (a) to prove that any product of three consecutive integers is a multiple of 3.

H 29. **a.** Use the quotient-remainder theorem with divisor equal to 3 to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.
b. Use the *mod* notation to rewrite the result of part (a).

30. **a.** Use the quotient-remainder theorem with divisor equal to 3 to prove that the product of any two consecutive integers has the form $3k$ or $3k + 2$ for some integer k.
b. Use the *mod* notation to rewrite the result of part (a).

In 31–33, you may use the properties listed in Example 4.3.3.

31. **a.** Prove that for all integers m and n, $m + n$ and $m - n$ are either both odd or both even.
b. Find all solutions to the equation $m^2 - n^2 = 56$ for which both m and n are positive integers.
c. Find all solutions to the equation $m^2 - n^2 = 88$ for which both m and n are positive integers.

32. Given any integers a, b, and c, if $a - b$ is even and $b - c$ is even, what can you say about the parity of $2a - (b + c)$? Prove your answer.

33. Given any integers a, b, and c, if $a - b$ is odd and $b - c$ is even, what can you say about the parity of $a - c$? Prove your answer.

H 34. Given any integer n, if $n > 3$, could n, $n + 2$, and $n + 4$ all be prime? Prove or give a counterexample.

Prove each of the statements in 35–43.

35. The fourth power of any integer has the form $8m$ or $8m + 1$ for some integer m.

H 36. The product of any four consecutive integers is divisible by 8.

H 37. For any integer n, $n^2 + 5$ is not divisible by 4.

38. For every integer m, $m^2 = 5k$, or $m^2 = 5k + 1$, or $m^2 = 5k + 4$ for some integer k.

H 39. Every prime number except 2 and 3 has the form $6q + 1$ or $6q + 5$ for some integer q.

40. If n is any odd integer, then $n^4 \ mod \ 16 = 1$.

H 41. For all real numbers x and y, $|x| \cdot |y| = |xy|$.

42. For all real numbers r and c with $c \geq 0$, $-c \leq r \leq c$ if, and only if, $|r| \leq c$. (*Hint:* Proving A if, and only if, B requires proving both if A then B and if B then A.)

H 43. For all real numbers a and b, $\big||a| - |b|\big| \leq |a - b|$.

44. A matrix $\mathbf{M}$ has 3 rows and 4 columns.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

The 12 entries in the matrix are to be stored in *row major* form in locations 7,609 to 7,620 in a computer's memory. This means that the entries in the first row (reading left to right) are stored first, then the entries in the second row, and finally the entries in the third row.
a. Which location will a_{22} be stored in?
b. Write a formula (in i and j) that gives the integer n so that a_{ij} is stored in location $7{,}609 + n$.
c. Find formulas (in n) for r and s so that a_{rs} is stored in location $7{,}609 + n$.

45. Let $\mathbf{M}$ be a matrix with m rows and n columns, and suppose that the entries of $\mathbf{M}$ are stored in a computer's memory in row major form (see exercise 44) in locations N, $N + 1$, $N + 2$, . . . , $N + mn - 1$. Find formulas in k for r and s so that a_{rs} is stored in location $N + k$.

*** 46.** If m, n, and d are integers, $d > 0$, and $m \ mod \ d = n \ mod \ d$, does it necessarily follow that $m = n$? That $m - n$ is divisible by d? Prove your answers.

* **47.** If m, n, and d are integers, $d > 0$, and $d|(m - n)$, what is the relation between $m \bmod d$ and $n \bmod d$? Prove your answer.

* **48.** If m, n, a, b, and d are integers, $d > 0$, and $m \bmod d = a$ and $n \bmod d = b$, is $(m + n) \bmod d = a + b$? Is $(m + n) \bmod d = (a + b) \bmod d$? Prove your answers.

* **49.** If m, n, a, b, and d are integers, $d > 0$, and $m \bmod d = a$ and $n \bmod d = b$, is $(mn) \bmod d = ab$? Is $(mn) \bmod d = ab \bmod d$? Prove your answers.

50. Prove that if m, d, and k are integers and $d > 0$, then $(m + dk) \bmod d = m \bmod d$.

ANSWERS FOR TEST YOURSELF

1. integers; $n = dq + r$; $0 \le r < d$ **2.** the quotient obtained when n is divided by d; the nonnegative remainder obtained when n is divided by d **3.** odd or even **4.** 0, 1, 2, . . . , $(d - 1)$; dq, $dq + 1$, $dq + 2$, . . . , $dq + (d - 1)$ **5.** If A_1, then C; If A_2, then C; If A_3, then C **6.** $|x + y| \le |x| + |y|$

4.6 Direct Proof and Counterexample VI: Floor and Ceiling

Proof serves many purposes simultaneously. In being exposed to the scrutiny and judgment of a new audience, [a] proof is subject to a constant process of criticism and revalidation. Errors, ambiguities, and misunderstandings are cleared up by constant exposure. Proof is respectability. Proof is the seal of authority.

Proof, in its best instances, increases understanding by revealing the heart of the matter. Proof suggests new mathematics. The novice who studies proofs gets closer to the creation of new mathematics. Proof is mathematical power, the electric voltage of the subject which vitalizes the static assertions of the theorems.

Finally, proof is ritual, and a celebration of the power of pure reason.

—Philip J. Davis and Reuben Hersh, *The Mathematical Experience*, 1981

Imagine a real number sitting on a number line. The *floor* and *ceiling* of the number are the integers to the immediate left and to the immediate right of the number (unless the number is an integer, in which case its floor and ceiling both equal the number itself). Many computer languages have built-in functions that compute floor and ceiling automatically. These functions are very convenient to use when writing certain kinds of computer programs. In addition, the concepts of floor and ceiling are important in analyzing the efficiency of many computer algorithms.

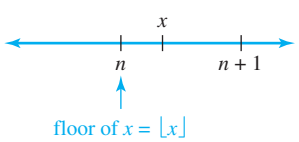
Definition

Given any real number x, the **floor of x**, denoted $\lfloor x \rfloor$, is defined as follows:

$$\lfloor x \rfloor = \text{that unique integer } n \text{ such that } n \le x < n + 1.$$

Symbolically, if x is a real number and n is an integer, then

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \le x < n + 1.$$



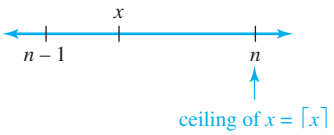
Definition

Given any real number x, the **ceiling of x**, denoted $\lceil x \rceil$, is defined as follows:

$$\lceil x \rceil = \text{that unique integer } n \text{ such that } n - 1 < x \leq n.$$

Symbolically, if x is a real number and n is an integer, then

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n.$$



Example 4.6.1 **Computing Floors and Ceilings**

Note On some calculators $\lfloor x \rfloor$ is denoted INT (x).

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the following values of x:

a. $25/4$ b. 0.999 c. -2.01

Solution

a. $25/4 = 6.25$ and $6 < 6.25 < 7$; hence $\lfloor 25/4 \rfloor = 6$ and $\lceil 25/4 \rceil = 7$.

b. $0 < 0.999 < 1$; hence $\lfloor 0.999 \rfloor = 0$ and $\lceil 0.999 \rceil = 1$.

c. $-3 < -2.01 < -2$; hence $\lfloor -2.01 \rfloor = -3$ and $\lceil -2.01 \rceil = -2$. ■

Example 4.6.2 **An Application**

The 1,370 students at a college are given the opportunity to take buses to an out-of-town event. Each bus holds a maximum of 40 passengers.

a. For reasons of economy, the leader of the event will send only full buses. What is the maximum number of buses the event leader will send?

b. If the event leader is willing to send one partially filled bus, how many buses will be needed to allow all the students to take the trip?

Solution

a. $\lfloor 1370/40 \rfloor = \lfloor 34.25 \rfloor = 34$ b. $\lceil 1370/40 \rceil = \lceil 34.25 \rceil = 35$ ■

Example 4.6.3 **Some General Values of Floor**

If k is an integer, what are $\lfloor k \rfloor$ and $\lfloor k + 1/2 \rfloor$? Why?

Solution Suppose k is an integer. Then

$$\lfloor k \rfloor = k \text{ because } k \text{ is an integer and } k \leq k < k + 1,$$

and

$$\left\lfloor k + \frac{1}{2} \right\rfloor = k \text{ because } k \text{ is an integer and } k \leq k + \frac{1}{2} < k + 1.$$ ■

Example 4.6.4 **Disproving an Alleged Property of Floor**

Is the following statement true or false?

For all real numbers x and y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$.

Solution The statement is false. As a counterexample, take $x = y = \frac{1}{2}$. Then

$$\lfloor x \rfloor + \lfloor y \rfloor = \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor = 0 + 0 = 0,$$

whereas

$$\lfloor x + y \rfloor = \left\lfloor \frac{1}{2} + \frac{1}{2} \right\rfloor = \lfloor 1 \rfloor = 1.$$

Hence it is not always the case that $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$.

To arrive at this counterexample, you could have reasoned as follows: Suppose x and y are real numbers. Must it necessarily be the case that $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$, or could x and y be such that $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$? Imagine values that the various quantities could take. For instance, if both x and y are positive, then $\lfloor x \rfloor$ and $\lfloor y \rfloor$ are the integer parts of $\lfloor x \rfloor$ and $\lfloor y \rfloor$ respectively; just as

$$2\frac{3}{5} = 2 + \frac{3}{5}$$

integer part fractional part

so is

$$x = \lfloor x \rfloor + \text{fractional part of } x$$

and

$$y = \lfloor y \rfloor + \text{fractional part of } y,$$

where the term *fractional part* is understood here to mean the part of the number to the right of the decimal point when the number is written in decimal notation. Thus if x and y are positive,

$$x + y = \lfloor x \rfloor + \lfloor y \rfloor + \textit{the sum of the fractional parts of } x \textit{ and } y.$$

But also

$$x + y = \lfloor x + y \rfloor + \textit{the fractional part of } (x + y).$$

These equations show that if there exist numbers x and y such that the sum of the fractional parts of x and y is at least 1, then a counterexample can be found. As previously indicated, there do exist such x and y; for instance, $x = \frac{1}{2}$ and $y = \frac{1}{2}$. ■

The analysis of Example 4.6.4 indicates that if x and y are positive and the sum of their fractional parts is less than 1, then $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$. In particular, if x is positive and m is a positive integer, then $\lfloor x + m \rfloor = \lfloor x \rfloor + \lfloor m \rfloor = \lfloor x \rfloor + m$. (The fractional part of m is 0; hence the sum of the fractional parts of x and m equals the fractional part of x, which is less than 1.) It turns out that you can use the definition of floor to show that this equation holds for every real number x and for every integer m.

Example 4.6.5 **Proving a Property of Floor**

Prove that for every real number x and for every integer m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Solution Begin by supposing that x is a particular but arbitrarily chosen real number and that m is a particular but arbitrarily chosen integer. You must show that $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. Since this is an equation involving $\lfloor x \rfloor$ and $\lfloor x + m \rfloor$, it is reasonable to give one of these quantities a name: Let $n = \lfloor x \rfloor$. By definition of floor,

$$n \text{ is an integer} \quad \text{and} \quad n \leq x < n + 1.$$

This double inequality enables you to compute the value of $\lfloor x + m \rfloor$ in terms of n by adding m to all sides:

$$n + m \leq x + m < n + m + 1.$$

Thus the left-hand side of the equation to be shown is

$$\lfloor x + m \rfloor = n + m.$$

On the other hand, since $n = \lfloor x \rfloor$, the right-hand side of the equation to be shown is

$$\lfloor x \rfloor + m = n + m$$

also. Thus $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. This discussion is summarized as follows:

Theorem 4.6.1

For every real number x and every integer m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof: Suppose any real number x and any integer m are given. *[We must show that* $\lfloor x + m \rfloor = \lfloor x \rfloor + m$*.]* Let $n = \lfloor x \rfloor$. By definition of floor, n is an integer and

$$n \leq x < n + 1.$$

Add m to all three parts to obtain

$$n + m \leq x + m < n + m + 1$$

[since adding a number to both sides of an inequality does not change the direction of the inequality].

Now $n + m$ is an integer *[since n and m are integers and a sum of integers is an integer]*, and so, by definition of floor, the left-hand side of the equation to be shown is

$$\lfloor x + m \rfloor = n + m.$$

But $n = \lfloor x \rfloor$. Hence, by substitution,

$$n + m = \lfloor x \rfloor + m,$$

which is the right-hand side of the equation to be shown. Thus $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ *[as was to be shown].*

■

The analysis of a number of computer algorithms, such as the binary search and merge sort algorithms, requires that you know the value of $\lfloor n/2 \rfloor$, where n is an integer. The formula for computing this value depends on whether n is even or odd.

Theorem 4.6.2 The Floor of $n/2$

For any integer n,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Proof: Suppose n is a *[particular but arbitrarily chosen]* integer. By the quotient-remainder theorem, either n is odd or n is even.

Case 1 (n is odd): In this case, $n = 2k + 1$ for some integer k. *[We must show that* $\lfloor n/2 \rfloor = (n-1)/2$*.]* But the left-hand side of the equation to be shown is

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

because k is an integer and $k \le k + 1/2 < k + 1$. And the right-hand side of the equation to be shown is

$$\frac{n-1}{2} = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k$$

also. So since both the left-hand and right-hand sides equal k, they are equal to each other. That is, $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ *[as was to be shown].*

Case 2 (n is even): In this case, $n = 2k$ for some integer k. *[We must show that* $\lfloor n/2 \rfloor = n/2$*.]* The rest of the proof of this case is left as an exercise.

Given any integer n and any positive integer d, the quotient-remainder theorem guarantees the existence of unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

The following theorem states that the floor notation can be used to describe q and r as follows:

$$q = \left\lfloor \frac{n}{d} \right\rfloor \quad \text{and} \quad r = n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor.$$

Thus if, on a calculator or in a computer language, floor is built in but *div* and *mod* are not, *div* and *mod* can be defined as follows: For a nonnegative integer n and a positive integer d,

$$n \text{ div } d = \left\lfloor \frac{n}{d} \right\rfloor \quad \text{and} \quad n \bmod d = n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor. \tag{4.6.1}$$

Note that d divides n if, and only if, $n \bmod d = 0$. In floor notation this means that d divides n if, and only if, $n = d \cdot \lfloor n/d \rfloor$. You are asked to prove this in exercise 33.

Theorem 4.6.3

If n is any integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d \cdot \lfloor n/d \rfloor$, then

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

Proof: Suppose n is any integer, d is a positive integer, $q = \lfloor n/d \rfloor$, and $r = n - d \cdot \lfloor n/d \rfloor$. *[We must show that $n = dq + r$ and $0 \le r < d$.]* By substitution,

$$dq + r = d \cdot \left\lfloor \frac{n}{d} \right\rfloor + \left(n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor \right) = n.$$

So it remains only to show that $0 \le r < d$. But $q = \lfloor n/d \rfloor$. Thus, by definition of floor,

$$q \le \frac{n}{d} < q + 1.$$

Then

$$dq \le n < dq + d \qquad \text{by multiplying all parts by } d$$

and so

$$0 \le n - dq < d \qquad \text{by subtracting } dq \text{ from all parts.}$$

But

$$r = n - d \left\lfloor \frac{n}{d} \right\rfloor = n - dq.$$

Hence

$$0 \le r < d \qquad \text{by substitution.}$$

[This is what was to be shown.]

Example 4.6.6 **Computing *div* and *mod***

Use the floor notation to compute 3,850 *div* 17 and 3,850 *mod* 17.

Solution By formula (4.6.1),

$$\begin{aligned} 3{,}850 \textit{ div } 17 &= \lfloor 3{,}850/17 \rfloor = \lfloor 226.4705882\ldots \rfloor = 226 \\ 3{,}850 \textit{ mod } 17 &= 3{,}850 - 17 \cdot \lfloor 3{,}850/17 \rfloor \\ &= 3{,}850 - 17 \cdot 226 \\ &= 3{,}850 - 3{,}842 = 8. \end{aligned}$$

■

TEST YOURSELF

1. Given any real number x, the floor of x is the unique integer n such that _____.
2. Given any real number x, the ceiling of x is the unique integer n such that _____.

EXERCISE SET 4.6

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the values of x in 1–4.

1. 37.999

2. $17/4$

3. -14.00001

4. $-32/5$

5. Use the floor notation to express 259 *div* 11 and 259 *mod* 11.

6. If k is an integer, what is $\lceil k \rceil$? Why?

7. If k is an integer, what is $\left\lceil k + \frac{1}{2} \right\rceil$? Why?

8. Seven pounds of raw material are needed to manufacture each unit of a certain product. Express the number of units that can be produced from n pounds of raw material using either the floor or the ceiling notation. Which notation is more appropriate?

9. Boxes, each capable of holding 36 units, are used to ship a product from the manufacturer to a wholesaler. Express the number of boxes that would be required to ship n units of the product using either the floor or the ceiling notation. Which notation is more appropriate?

10. If 0 = Sunday, 1 = Monday, 2 = Tuesday, . . . , 6 = Saturday, then January 1 of year n occurs on the day of the week given by the following formula:

$$\left(n + \left\lfloor \frac{n-1}{4} \right\rfloor - \left\lfloor \frac{n-1}{100} \right\rfloor + \left\lfloor \frac{n-1}{400} \right\rfloor\right) \textit{mod } 7.$$

a. Use this formula to find January 1 of
i. 2050 ii. 2100 iii. the year of your birth.

***H* b.** Interpret the different components of this formula.

11. State a necessary and sufficient condition for the floor of a real number to equal that number.

***H* 12.** Let S be the statement: For any odd integer n, $\lfloor n/2 \rfloor = (n-1)/2$. Then S is true, but the following "proof" is incorrect. Find the mistake.

"**Proof:** Suppose n is any odd integer. Then $n = 2k + 1$ for some integer k. Consequently,

$$\left\lfloor \frac{2k+1}{2} \right\rfloor = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k.$$

But $n = 2k + 1$. Solving for k gives $k = (n-1)/2$. Hence, by substitution, $\lfloor n/2 \rfloor = (n-1)/2$."

13. Prove that if n is any even integer, then $\lfloor n/2 \rfloor = n/2$.

14. Show that the following statement is false.

For all real numbers x and y, $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$.

Some of the statements in 15–22 are true and some are false. Prove each true statement and find a counterexample for each false statement, but do not use Theorem 4.6.1 in your proofs.

15. For every real number x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$.

16. For every real number x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

***H* 17.** For every integer n,

$$\lfloor n/3 \rfloor = \begin{cases} n/3 & \text{if } n \textit{ mod } 3 = 0 \\ (n-1)/3 & \text{if } n \textit{ mod } 3 = 1 \\ (n-2)/3 & \text{if } n \textit{ mod } 3 = 2. \end{cases}$$

***H* 18.** For all real numbers x and y, $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.

***H* 19.** For every real number x, $\lceil x - 1 \rceil = \lceil x \rceil - 1$.

20. For all real numbers x and y, $\lceil xy \rceil = \lceil x \rceil \cdot \lceil y \rceil$.

21. For every odd integer n, $\lceil n/2 \rceil = (n+1)/2$.

22. For all real numbers x and y, $\lceil xy \rceil = \lceil x \rceil \cdot \lfloor y \rfloor$.

Prove each of the statements in 23–33.

23. For any real number x, if x is not an integer, then $\lfloor x \rfloor + \lfloor -x \rfloor = -1$.

24. For any integer m and any real number x, if x is not an integer, then $\lfloor x \rfloor + \lfloor m - x \rfloor = m - 1$.

***H* 25.** For every real number x, $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor x/4 \rfloor$.

26. For every real number x, if $x - \lfloor x \rfloor < 1/2$ then $\lfloor 2x \rfloor = 2\lfloor x \rfloor$.

27. For every real number x, if $x - \lfloor x \rfloor \geq 1/2$ then $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$.

***H* 28.** For any odd integer n,

$$\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right).$$

29. For any odd integer n,

$$\left\lceil \frac{n^2}{4} \right\rceil = \frac{n^2+3}{4}.$$

***H* 30.** For every integer n, $\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n$.

***H* 31.** For every integer n, $\left\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{3} \right\rfloor = \left\lfloor \frac{n}{6} \right\rfloor$.

32. For every integer n, $\left\lceil \frac{\lceil \frac{n}{2} \rceil}{3} \right\rceil = \left\lceil \frac{n}{6} \right\rceil$.

33. A necessary and sufficient condition for an integer n to be divisible by a nonzero integer d is that $n = \lfloor n/d \rfloor \cdot d$. In other words, for every integer n and nonzero integer d,
a. if $d|n$, then $n = \lfloor n/d \rfloor \cdot d$.
b. if $n = \lfloor n/d \rfloor \cdot d$ then $d|n$.

ANSWERS FOR TEST YOURSELF

1. $n \le x < n+1$ **2.** $n-1 < x \le n$

4.7 Indirect Argument: Contradiction and Contraposition

Reductio ad absurdum . . . *is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but the mathematician offers the game.* —G. H. Hardy, 1877–1947

In a direct proof you start with the hypothesis of a statement and make one deduction after another until you reach the conclusion. Indirect proofs are more roundabout. One kind of indirect proof, *argument by contradiction*, is based on the fact that either a statement is true or it is false but not both. So if you can show that the assumption that a given statement is not true leads logically to a contradiction, impossibility, or absurdity, then that assumption must be false: and, hence, the given statement must be true. This method of proof is also known as *reductio ad impossible* or *reductio ad absurdum* because it relies on reducing a given assumption to an impossibility or absurdity.

Argument by contradiction occurs in many different settings. For example, if a man accused of holding up a bank can prove that he was someplace else at the time the crime was committed, he will certainly be acquitted. The logic of his defense is as follows:

> Suppose I did commit the crime. Then at the time of the crime, I would have had to be at the scene of the crime. In fact, at the time of the crime I was in a meeting with 20 people far from the crime scene, as they will testify. This contradicts the supposition that I committed the crime since it is impossible to be in two places at one time. Hence that supposition is false.

Another example occurs in debate. One technique of debate is to say, "Suppose for a moment that what my opponent says is correct." Starting from this supposition, the debater then deduces one statement after another until finally arriving at a statement that is completely ridiculous and unacceptable to the audience. By this means the debater shows the opponent's statement to be false.

The point of departure for a proof by contradiction is the supposition that the statement to be proved is false. The goal is to reason to a contradiction. Thus proof by contradiction has the following outline:

Caution! People often make mistakes when they write a negation for a statement they want to prove by contradiction.

Method of Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

There are no clear-cut rules for when to try a direct proof and when to try a proof by contradiction, but there are some general guidelines. Proof by contradiction is indicated if you want to show that there is no object with a certain property, or if you want to show that a certain object does not have a certain property. The next three examples illustrate these situations.

Example 4.7.1 **There Is No Greatest Integer**

Use proof by contradiction to show that there is no greatest integer.

Solution For this proof, the "certain property" is the property of being the greatest integer. So prove that there is no object with this property, begin by supposing the negation: that there is an object with the property.

Starting Point: Suppose not. Suppose there is a greatest integer; call it N. This means that $N \geq n$ for every integer n.

To Show: This supposition leads logically to a contradiction.

Theorem 4.7.1

There is no greatest integer.

Proof: *[We take the negation of the theorem and suppose it to be true.]* Suppose not. That is, suppose there is a greatest integer N. *[We must deduce a contradiction.]* Then $N \geq n$ for every integer n. Let $M = N + 1$. Now M is an integer since it is a sum of integers. Also $M > N$ since $M = N + 1$. Thus M is an integer that is greater than N. So N is the greatest integer and N is not the greatest integer, which is a contradiction. *[This contradiction shows that the supposition is false and, hence, that the theorem is true.]*

■

After a contradiction has been reached, the logic of the argument is always the same: "This is a contradiction. Hence the supposition is false and the theorem is true." Because of this, most mathematics texts end proofs by contradiction at the point at which the contradiction has been obtained.

The contradiction in the next example is based on the fact that $1/2$ is not an integer.

Example 4.7.2 **No Integer Can Be Both Even and Odd**

The fact that no integer is both even and odd can also be deduced from the uniqueness part of the quotient-remainder theorem. A full proof of this part of the theorem is outlined in exercise 21 of Section 4.8.

Theorem 4.7.2

There is no integer that is both even and odd.

Proof: *[We take the negation of the theorem and suppose it to be true.]* Suppose not. That is, suppose there is at least one integer n that is both even and odd.

(continued on page 220)

[We must deduce a contradiction.] By definition of even, $n = 2a$ for some integer a, and by definition of odd, $n = 2b + 1$ for some integer b. Consequently,

$$2a = 2b + 1 \quad \text{by equating the two expressions for } n,$$

and so

$$\begin{aligned} 2a - 2b &= 1 \\ 2(a - b) &= 1 \\ a - b &= 1/2 \quad \text{by algebra.} \end{aligned}$$

Now since a and b are integers, the difference $a - b$ must also be an integer. But $a - b = 1/2$, and $1/2$ is not an integer. Thus $a - b$ is an integer and $a - b$ is not an integer, which is a contradiction. *[This contradiction shows that the supposition is false and, hence, that the theorem is true.]*

■

If you want to prove that a certain object does not have a certain property, you may need to assume that it does have the property and deduce a contradiction. The next example illustrates this strategy. It asks you to prove that a certain object (the sum of a rational and an irrational number) does not have the property being rational.

Example 4.7.3 **The Sum of a Rational Number and an Irrational Number**

Use proof by contradiction to show that the sum of any rational number and any irrational number is irrational.

Caution! The negation of "The sum of any irrational number and any rational number is irrational" is NOT "The sum of any irrational number and any rational number is rational."

Solution Begin by supposing the negation of what you are to prove. Be very careful when writing down what this means. If you take the negation incorrectly, the entire rest of the proof will be flawed. In this example, the statement to be proved can be written formally as

$$\forall \text{ real numbers } r \text{ and } s, \text{ if } r \text{ is rational and } s \text{ is irrational, then } r + s \text{ is irrational.}$$

From this you can see that the negation is

$$\exists \text{ a rational number } r \text{ and an irrational number } s \text{ such that } r + s \text{ is rational.}$$

It follows that the starting point and what is to be shown are as follows:

Starting Point: Suppose not. That is, suppose there is a rational number r and an irrational number s such that $r + s$ is rational.

To Show: This supposition leads to a contradiction.

To derive a contradiction, you need to understand what you are supposing: that there are numbers r and s such that r is rational, s is irrational, and $r + s$ is rational. By definition of rational and irrational, this means there are convenient expressions that can be substituted for r and $r + s$, but all you can say about s is that it cannot be written as a quotient of integers

$$r = \frac{a}{b} \quad \text{for some integers } a \text{ and } b \text{ with } b \neq 0, \text{ and} \qquad 4.7.1$$

$$r + s = \frac{c}{d} \quad \text{for some integers } c \text{ and } d \text{ with } d \neq 0. \qquad 4.7.2$$

Note There is no convenient expression that can be substituted for an irrational number.

If you substitute (4.7.1) into (4.7.2), you obtain

$$\frac{a}{b} + s = \frac{c}{d}.$$

Subtracting a/b from both sides gives

$$\begin{aligned} s &= \frac{c}{d} - \frac{a}{b} \\ &= \frac{bc}{bd} - \frac{ad}{bd} && \text{by rewriting } c/d \text{ and } a/b \text{ as equivalent fractions} \\ &= \frac{bc - ad}{bd} && \text{by the rule for subtracting fractions with the same denominator.} \end{aligned}$$

Now both $bc - ad$ and bd are integers because products and differences of integers are integers, and $bd \neq 0$ by the zero product property. Hence s can be expressed as a quotient of two integers with a nonzero denominator, and so s is rational, which contradicts the supposition that it is irrational.

This discussion is summarized in a formal proof.

Theorem 4.7.3

The sum of any rational number and any irrational number is irrational.

Proof:

[We take the negation of the theorem and suppose it to be true.] Suppose not. That is, suppose there is a rational number r and an irrational number s such that $r + s$ is rational. *[We must deduce a contradiction.]* By definition of rational, $r = a/b$ and $r + s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. By substitution,

$$\frac{a}{b} + s = \frac{c}{d},$$

and so

$$\begin{aligned} s &= \frac{c}{d} - \frac{a}{b} && \text{by subtracting } a/b \text{ from both sides} \\ &= \frac{bc - ad}{bd} && \text{by the laws of algebra.} \end{aligned}$$

Now $bc - ad$ and bd are both integers *[since a, b, c, and d are integers and since products and differences of integers are integers]*, and $bd \neq 0$ *[by the zero product property]*. Hence s is a quotient of the two integers $bc - ad$ and bd with $bd \neq 0$. Thus, by definition of rational, s is rational, which contradicts the supposition that s is irrational. *[Hence the supposition is false and the theorem is true.]*

■

Argument by Contraposition

A second form of indirect argument, *argument by contraposition*, is based on the logical equivalence between a statement and its contrapositive. To prove a statement by contraposition, you take the contrapositive of the statement, prove the contrapositive by a direct proof, and conclude that the original statement is true. The underlying reasoning is that

since a conditional statement is logically equivalent to its contrapositive, if the contrapositive is true then the statement must also be true.

Method of Proof by Contraposition

1. Express the statement to be proved in the form

   $$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

   (This step may be done mentally.)
2. Rewrite this statement in the contrapositive form

   $$\forall x \text{ in } D, \text{ if } Q(x) \text{ is false then } P(x) \text{ is false.}$$

   (This step may also be done mentally.)
3. Prove the contrapositive by a direct proof.
   a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.
   b. Show that $P(x)$ is false.

Example 4.7.4 **If the Square of an Integer Is Even, Then the Integer Is Even**

Prove that for every integer n, if n^2 is even then n is even.

Solution First form the contrapositive of the statement to be proved.

Contrapositive: For every integer n, if n is not even then n^2 is not even.

By the quotient-remainder theorem with divisor equal to 2, any integer is even or odd, and, by Theorem 4.7.2, no integer is both even and odd. So if an integer is not even, then it is odd. Thus the contrapositive can be restated as follows:

Contrapositive: For every integer n, if n is odd then n^2 is odd.

A straightforward computation is the heart of a direct proof for this statement, as shown below.

Proposition 4.7.4

For every integer n, if n^2 is even then n is even.

Proof (by contraposition): Suppose n is any odd integer. *[We must show that n^2 is odd.]* By definition of odd, $n = 2k + 1$ for some integer k. By substitution and algebra,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Now $2k^2 + 2k$ is an integer because products and sums of integers are integers. So $n^2 = 2 \cdot (\text{an integer}) + 1$, and thus, by definition of odd, n^2 is odd *[as was to be shown].*

We used the word *proposition* here rather than *theorem* because although the word *theorem* can refer to any statement that has been proved, mathematicians often restrict it to especially important statements that have many and varied consequences. Then they use

the word **proposition** to refer to a statement that is somewhat less consequential but nonetheless worth writing down. We will use Proposition 4.7.4 in Section 4.8 to prove that $\sqrt{2}$ is irrational. ■

Relation between Proof by Contradiction and Proof by Contraposition

Observe that any proof by contraposition can be recast in the language of proof by contradiction. In a proof by contraposition, the statement

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x)$$

is proved by giving a direct proof of the equivalent statement

$$\forall x \text{ in } D, \text{ if } \sim Q(x) \text{ then } \sim P(x).$$

To do this, you suppose you are given an arbitrary element x of D such that $\sim Q(x)$. You then show that $\sim P(x)$. This is illustrated in Figure 4.7.1.

FIGURE 4.7.1 Proof by Contraposition

Exactly the same sequence of steps can be used as the heart of a proof by contradiction for the given statement. The only thing that changes is the context in which the steps are written down.

To rewrite the proof as a proof by contradiction, you suppose there is an x in D such that $P(x)$ and $\sim Q(x)$. You then follow the steps of the proof by contraposition to deduce the statement $\sim P(x)$. But $\sim P(x)$ is a contradiction to the supposition that $P(x)$ and $\sim Q(x)$. (Because to contradict a conjunction of two statements, it is only necessary to contradict one of them.) This process is illustrated in Figure 4.7.2.

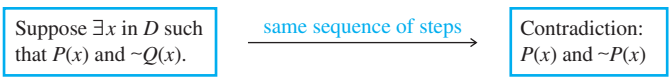


FIGURE 4.7.2 Proof by Contradiction

As an example, here is a proof by contradiction of Proposition 4.7.4.

Proposition 4.7.4

For every integer n, if n^2 is even then n is even.

Proof (by contradiction): *[We take the negation of the theorem and suppose it to be true.]* Suppose not. That is, suppose there is an integer n such that n^2 is even and n is not even. *[We must deduce a contradiction.]* By the quotient-remainder theorem with divisor equal to 2, any integer is even or odd. Hence, since n is not even it is odd, and thus, by definition of odd, $n = 2k + 1$ for some integer k. By substitution and algebra,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

(continued on page 224)

Now $2k^2 + 2k$ is an integer because products and sums of integers are integers. So $n^2 = 2 \cdot$(an integer) $+ 1$, and thus, by definition of odd, n^2 is odd. Therefore, n^2 is both even and odd. This contradicts Theorem 4.7.2, which states that no integer can be both even and odd. *[This contradiction shows that the supposition is false and, hence, that the proposition is true.]*

Note that when you use proof by contraposition, you know exactly what conclusion you need to show, namely, the negation of the hypothesis; whereas in proof by contradiction, it may be difficult to know what contradiction to head for. On the other hand, when you use proof by contradiction, once you have deduced any contradiction whatsoever, you are done. The main advantage of contraposition over contradiction is that you avoid having to take (possibly incorrectly) the negation of a complicated statement. The disadvantage of contraposition as compared with contradiction is that you can use contraposition only for a specific class of statements—those that are universal and conditional. The previous discussion shows that any statement that can be proved by contraposition can be proved by contradiction. But the converse is not true. Statements such as "$\sqrt{2}$ is irrational" (discussed in the next section) can be proved by contradiction but not by contraposition.

Proof as a Problem-Solving Tool

Direct proof, disproof by counterexample, proof by contradiction, and proof by contraposition are all tools that may be used to help determine whether statements are true or false. Working with examples might have given you a sense that a statement of the form

For all elements in a domain, if (hypothesis) then (conclusion),

might be true. To explore further, imagine elements in the domain that satisfy the hypothesis. Ask yourself: Must they satisfy the conclusion? If you can see that the answer is "yes" in all cases, then the statement is true and your insight will form the basis for a direct proof. If after some thought it is not clear that the answer is "yes," ask yourself whether there are elements of the domain that satisfy the hypothesis and *not* the conclusion. If you are successful in finding some, then the statement is false and you have a counterexample. On the other hand, if you are not successful in finding such elements, perhaps none exist. Perhaps you can show that assuming the existence of elements in the domain that satisfy the hypothesis and not the conclusion leads logically to a contradiction. If so, then the given statement is true and you have the basis for a proof by contradiction. Alternatively, you could imagine elements of the domain for which the conclusion is false and ask whether such elements also fail to satisfy the hypothesis. If the answer in all cases is "yes," then you have a basis for a proof by contraposition.

Solving problems, especially difficult problems, is rarely a straightforward process. At any stage of following the guidelines above, you might want to try the method of a previous stage again. If, for example, you fail to find a counterexample for a certain statement, your experience in trying to find it might help you decide to reattempt a direct argument rather than trying an indirect one. Psychologists who have studied problem solving have found that the most successful problem solvers are those who are flexible and willing to use a variety of approaches without getting stuck in any one of them for very long. Mathematicians sometimes work for months (or longer) on difficult problems. Don't be discouraged if some problems in this book take you quite a while to solve.

Learning the skills of proof and disproof is much like learning other skills, such as those used in a sport or playing a musical instrument. When you first start out, you may

feel bewildered by all the rules, and you may not feel confident as you attempt new things. But with practice the rules become internalized and you can use them in conjunction with all your other powers—of balance, coordination, judgment, aesthetic sense—to concentrate on winning a competition or performing in public.

Now that you have worked through several sections of this chapter, return to the idea that, above all, a proof or disproof should be a convincing argument. You need to know how direct and indirect proofs and counterexamples are structured. But to use this knowledge effectively, you must use it in conjunction with your imaginative powers, your intuition, and especially your common sense.

TEST YOURSELF

1. To prove a statement by contradiction, you suppose that _____ and you show that _____.
2. A proof by contraposition of a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" is a direct proof of _____.
3. To prove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" by contraposition, you suppose that _____ and you show that _____.

EXERCISE SET 4.7

1. Fill in the blanks in the following proof by contradiction that there is no least positive real number.

   Proof: Suppose not. That is, suppose that there is a least positive real number x. *[We must deduce* __(a)__ *]* Consider the number $x/2$. Since x is a positive real number, $x/2$ is also __(b)__. In addition, we can deduce that $x/2 < x$ by multiplying both sides of the inequality $1 < 2$ by __(c)__ and dividing __(d)__. Hence $x/2$ is a positive real number that is less than the least positive real number. This is a __(e)__. *[Thus the supposition is false, and so there is no least positive real number.]*

2. Is $\frac{1}{0}$ an irrational number? Explain.
3. Use proof by contradiction to show that for every integer n, $3n + 2$ is not divisible by 3.
4. Use proof by contradiction to show that for every integer m, $7m + 4$ is not divisible by 7.

Carefully formulate the negations of each of the statements in 5–7. Then prove each statement by contradiction.

5. There is no greatest even integer.
6. There is no greatest negative real number.
7. There is no least positive rational number.
8. Fill in the blanks for the following proof that the difference of any rational number and any irrational number is irrational.

   Proof (by contradiction): Suppose not. That is, suppose that there exist __(a)__ x and __(b)__ y such that $x - y$ is rational. By definition of rational, there exist integers a, b, c, and d with $b \neq 0$ and $d \neq 0$ so that $x =$ __(c)__ and $x - y =$ __(d)__. By substitution,

   $$\frac{a}{b} - y = \frac{c}{d}$$

   Adding y and subtracting $\frac{c}{d}$ on both sides gives

   $$\begin{aligned} y &= \text{(e)} && \text{by substitution} \\ &= \frac{ad}{bd} - \frac{bc}{bd} \\ &= \frac{ad - bc}{bd} && \text{by algebra.} \end{aligned}$$

   Now both $ad - bc$ and bd are integers because products and differences of __(f)__ are __(g)__. And $bd \neq 0$ by the __(h)__. Hence y is a ratio of integers with a nonzero denominator, and thus y is __(i)__ by definition of rational. We therefore have both that y is irrational and that y is rational, which is a contradiction. *[Thus the supposition is false and the statement to be proved is true.]*

9. **a.** When asked to prove that the difference of any irrational number and any rational number is irrational, a student began, "Suppose not. That is, suppose the difference of any irrational number and any rational number is rational."

What is wrong with beginning the proof in this way? (*Hint:* If needed, review the answer to exercise 11 in Section 3.2.)

b. Prove that the difference of any irrational number and any rational number is irrational.

10. Let S be the statement: For all positive real numbers r and s, $\sqrt{r+s} \neq \sqrt{r}+\sqrt{s}$. Statement S is true, but the following "proof" is incorrect. Find the mistake.

"**Proof by contradiction:** Suppose not. That is, suppose that for all positive real numbers r and s, $\sqrt{r+s} = \sqrt{r}+\sqrt{s}$. This means that the equation will be true no matter what positive real numbers are substituted for r and s. So let $r = 9$ and $s = 16$. Then r and s are positive real numbers and

$$\sqrt{r+s} = \sqrt{9+16} = \sqrt{25} = 5$$

whereas

$$\sqrt{r}+\sqrt{s} = \sqrt{9}+\sqrt{16} = 3+4 = 7.$$

Since $5 \neq 7$, we have that $\sqrt{r+s} \neq \sqrt{r}+\sqrt{s}$, which contradicts the supposition that $\sqrt{r+s} = \sqrt{r}+\sqrt{s}$. This contradiction shows that the supposition is false, and hence statement S is true."

11. Let T be the statement: The sum of any two rational numbers is rational. Then T is true, but the following "proof" is incorrect. Find the mistake.

"**Proof by contradiction:** Suppose not. That is, suppose that the sum of any two rational numbers is not rational. This means that no matter what two rational numbers are chosen their sum is not rational. Now both 1 and 3 are rational because $1 = 1/1$ and $3 = 3/1$, and so both are ratios of integers with a nonzero denominator. Hence, by a supposition, the sum of 1 and 3, which is 4, is not rational. But 4 is rational because $4 = 4/1$, which is a ratio of integers with a nonzero denominator. Hence 4 is both rational and not rational, which is a contradiction. This contradiction shows that the supposition is false, and hence statement T is true."

12. Let R be the statement: The square root of any irrational number is irrational.

a. Write a negation for R.

b. Prove R by contradiction.

13. Let S be the statement: The product of any irrational number and any nonzero rational number is irrational.

a. Write a negation for S.

b. Prove S by contradiction.

14. Let T be the statement: For every integer a, if $a \bmod 6 = 3$, then $a \bmod 3 \neq 2$.

a. Write a negation for T.

H **b.** Prove T by contradiction.

H **15.** Do there exist integers a, b, and c such that a, b, and c are all odd and $a^2 + b^2 = c^2$? Prove your answer.

Prove each statement in 16–19 by contradiction.

16. For all odd integers a and b, $b^2 - a^2 \neq 4$. (*Hint:* $b^2 - a^2 = (b+a)(b-a)$ and the only way to factor 4 is either $4 = 2 \cdot 2$ or $4 = 4 \cdot 1$.)

H **17.** For all prime numbers a, b, and c, $a^2 + b^2 \neq c^2$.

18. If a and b are rational numbers, $b \neq 0$, and r is an irrational number, then $a + br$ is irrational.

H **19.** For any integer n, $n^2 - 2$ is not divisible by 4.

20. Fill in the blanks in the following proof by contraposition that for every integer n, if $5 \nmid n^2$ then $5 \nmid n$.

Proof (by contraposition): *[The contrapositive is: For every integer n, if* $5 \mid n$ *then* $5 \mid n^2$*.]* Suppose n is any integer such that ___(a)___. *[We must show that* ___(b)___*.]* By definition of divisibility, $n =$ ___(c)___ for some integer k. By substitution, $n^2 =$ ___(d)___ $= 5(5k^2)$. But $5k^2$ is an integer because it is a product of integers. Hence $n^2 = 5 \cdot$(an integer), and so ___(e)___ *[as was to be shown].*

21. Consider the statement "For every integer n, if n^2 is odd then n is odd."

a. Write what you would suppose and what you would need to show to prove this statement by contradiction.

b. Write what you would suppose and what you would need to show to prove this statement by contraposition.

22. Consider the statement "For every real number r, if r^2 is irrational then r is irrational."

a. Write what you would suppose and what you would need to show to prove this statement by contradiction.

b. Write what you would suppose and what you would need to show to prove this statement by contraposition.

Prove each of the statements in 23–25 in two ways: (a) by contraposition and (b) by contradiction.

23. The negative of any irrational number is irrational.

24. The reciprocal of any irrational number is irrational. (The **reciprocal** of a nonzero real number x is $1/x$.)

H 25. For every integer n, if n^2 is odd then n is odd.

Use any method to prove the statements in 26–29.

26. For all integers a, b, and c, if $a \nmid bc$ then $a \nmid b$.

27. For all positive real numbers r and s, $\sqrt{r+s} \neq \sqrt{r} + \sqrt{s}$.

H 28. For all integers a, b, and c, if $a \mid b$ and $a \nmid c$, then $a \nmid (b+c)$.

H 29. For all integers m and n, if $m+n$ is even then m and n are both even or m and n are both odd.

30. a. Let $n = 53$. Find an approximate value for $\sqrt{n}$ and write a list of all the prime numbers less than or equal to $\sqrt{n}$. Is the following statement true or false? When $n = 53$, n is not divisible by any prime number less than or equal to $\sqrt{n}$.

b. Suppose n is a fixed integer. Let S be the statement, "n is not divisible by any prime number less than or equal to $\sqrt{n}$." The following statement is equivalent to S:

$\forall$ prime number p, if p is less than or equal to $\sqrt{n}$ then n is not divisible by p.

Which of the following are negations for S?

(i) $\exists$ a prime number p such that $p \leq \sqrt{n}$ and n is divisible by p.
(ii) n is divisible by every prime number less than or equal to $\sqrt{n}$.
(iii) $\exists$ a prime number p such that p is a multiple of n and p is less than or equal to $\sqrt{n}$.
(iv) n is divisible by some prime number that is less than or equal to $\sqrt{n}$.
(v) $\forall$ prime number p, if p is less than or equal to $\sqrt{n}$, then n is divisible by p.

31. a. Prove by contraposition: For all positive integers n, r, and s, if $rs \leq n$, then $r \leq \sqrt{n}$ or $s \leq \sqrt{n}$.

(*Hint:* Use Theorem T27 in Appendix A.)

b. Prove: For each integer $n > 1$, if n is not prime then there exists a prime number p such that $p \leq \sqrt{n}$ and n is divisible by p. (*Hint:* Use the results of part (a), Theorems 4.4.1, 4.4.3, and 4.4.4, and the transitive property of order.)

c. State the contrapositive of the result of part (b). The results of exercise 31 provide a way to test whether an integer is prime.

Test for Primality

Given an integer $n > 1$, to test whether n is prime check to see if it is divisible by a prime number less than or equal to its square root. If it is not divisible by any of these numbers, then it is prime.

32. Use the test for primality to determine whether the following numbers are prime or not.

a. 667 **b.** 557 **c.** 527 **d.** 613

33. The sieve of Eratosthenes, named after its inventor, the Greek scholar Eratosthenes (276–194 B.C.E.), provides a way to find all prime numbers less han or equal to some fixed number n. To construct it, write out all the integers from 2 to n. Cross out all multiples of 2 except 2 itself, then all multiples of 3 except 3 itself, then all multiples of 5 except 5 itself, and so forth. Continue crossing out the multiples of each successive prime number up to $\sqrt{n}$. The numbers that are not crossed out are all the prime numbers from 2 to n. Here is a sieve of Eratosthenes that includes the numbers from 2 to 27. The multiples of 2 are crossed out with a /, the multiples of 3 with a \, and the multiples of 5 with a —.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~
~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~

Use the sieve of Eratosthenes to find all prime numbers less than 100.

34. Use the test for primality and the result of exercise 33 to determine whether the following numbers are prime.

a. 9,269 **b.** 9,103 **c.** 8,623 **d.** 7,917

H* 35. Use proof by contradiction to show that every integer greater than 11 is a sum of two composite numbers.

H* 36. For all odd integers a, b, and c, if z is a solution of $ax^2 + bx + c = 0$ then z is irrational. (In the proof, use the properties of even and odd integers that are listed in Example 4.3.3.)

ANSWERS FOR TEST YOURSELF

1. the statement is false; this supposition leads to a contradiction **2.** the contrapositive of the statement, namely, $\forall x \in D$, if $\sim Q(x)$ then $\sim P(x)$ **3.** x is any *[particular but arbitrarily chosen]* element of D for which $Q(x)$ is false; $P(x)$ is false

4.8 Indirect Argument: Two Famous Theorems

He is unworthy of the name of man who does not know that the diagonal of a square is incommensurable with its side. —Plato (ca. 428–347 B.C.E.)

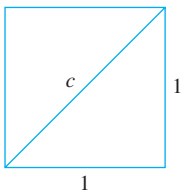
This section contains proofs of two of the most famous theorems in mathematics: that $\sqrt{2}$ is irrational and that there are infinitely many prime numbers. Both proofs are examples of indirect arguments and were well known more than 2,000 years ago, but they remain exemplary models of mathematical argument to this day.

The Irrationality of $\sqrt{2}$

When mathematics flourished at the time of the ancient Greeks, mathematicians believed that given any two line segments, say A: _____ and B: _____, a certain unit of length could be found so that segment A was exactly m units long and segment B was exactly n units long, for some integers m and n. (The segments were said to be *commensurable* with respect to this special unit of length.) Then the ratio of the lengths of A and B would be in the same proportion as the ratio of the integers m and n. Symbolically:

$$\frac{\text{length } A}{\text{length } B} = \frac{m}{n}.$$

Now it is easy to find a line segment of length $\sqrt{2}$; just take the diagonal of a unit square:



By the Pythagorean theorem, $c^2 = 1^2 + 1^2 = 2$, and so $c = \sqrt{2}$. If the belief of the ancient Greeks were correct, there would be integers m and n such that

$$\frac{\text{length (diagonal)}}{\text{length (side)}} = \frac{m}{n}.$$

And this would imply that

$$\frac{c}{1} = \frac{\sqrt{2}}{1} = \sqrt{2} = \frac{m}{n}.$$

But then $\sqrt{2}$ would be a ratio of two integers, or, in other words, $\sqrt{2}$ would be rational.

In the fourth or fifth century B.C.E., the followers of the Greek mathematician and philosopher Pythagoras discovered that $\sqrt{2}$ was not rational. This discovery was very upsetting to them, for it undermined their deep, quasi-religious belief in the power of whole numbers to describe phenomena.

Bettmann/Getty Images

Euclid
(fl. 300 B.C.E.)

The following proof of the irrationality of $\sqrt{2}$ was known to Aristotle and is similar to that in the tenth book of Euclid's *Elements of Geometry*. The Greek mathematician Euclid is best known as a geometer, and knowledge of the geometry in the first six books of his *Elements* was considered an essential part of a liberal education for more than 2,000 years. However, books 7–10 of his *Elements* contain much that we would now call number theory.

The proof begins by supposing the negation: $\sqrt{2}$ is rational. This means that there exist integers m and n such that $\sqrt{2} = m/n$. Now if m and n have any common factors, these may be factored out to obtain a new fraction, equal to m/n, in which the numerator and denominator have no common factors. (For example, $18/12 = (6 \cdot 3)/(6 \cdot 2) = 3/2$, which is a fraction whose numerator and denominator have no common factors.) Thus, without loss of generality, we may assume that m and n had no common factors in the first place. We will then derive the contradiction that m and n *do* have a common factor of 2. The argument makes use of Proposition 4.7.4: If the square of an integer is even, then that integer is even.

Note Strictly speaking, being able to assume that m and n have no common factors is a consequence of the "well-ordering principle for the integers," which is discussed in Section 5.4.

Theorem 4.8.1 Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational.

Proof (by contradiction): *[We take the negation and suppose it to be true.]* Suppose not. That is, suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors such that

$$\sqrt{2} = \frac{m}{n} \tag{4.8.1}$$

[by dividing m and n by any common factors if necessary]. [We must derive a contradiction.] Squaring both sides of equation (4.8.1) gives

$$2 = \frac{m^2}{n^2}.$$

Or, equivalently,

$$m^2 = 2n^2. \tag{4.8.2}$$

Note that equation (4.8.2) implies that m^2 is even (by definition of even). It follows that m is even (by Proposition 4.7.4). We file this fact away for future reference and also deduce (by definition of even) that

$$m = 2k \quad \text{for some integer } k. \tag{4.8.3}$$

Substituting equation (4.8.3) into equation (4.8.2), we see that

$$m^2 = (2k)^2 = 4k^2 = 2n^2.$$

Dividing both sides of the right-most equation by 2 gives

$$n^2 = 2k^2.$$

Consequently, n^2 is even, and so n is even (by Proposition 4.7.4). But we also know that m is even. *[This is the fact we filed away.]* Hence both m and n have a common factor of 2. But this contradicts the supposition that m and n have no common factors. *[Hence the supposition is false and so the theorem is true.]*

Now that you have seen the proof that $\sqrt{2}$ is irrational, you can use the irrationality of $\sqrt{2}$ to derive the irrationality of certain other real numbers.

Example 4.8.1 **Irrationality of $1 + 3\sqrt{2}$**

Prove by contradiction that $1 + 3\sqrt{2}$ is irrational.

Solution The essence of the argument is the observation that if $1 + 3\sqrt{2}$ could be written as a ratio of integers, then so could $\sqrt{2}$. But by Theorem 4.8.1, we know that to be impossible.

Proposition 4.8.2

$1 + 3\sqrt{2}$ is irrational.

Proof: Suppose not. Suppose $1 + 3\sqrt{2}$ is rational. *[We must derive a contradiction.]* Then by definition of rational,

$$1 + 3\sqrt{2} = \frac{a}{b} \quad \text{for some integers } a \text{ and } b \text{ with } b \neq 0.$$

It follows that

$$\begin{aligned} 3\sqrt{2} &= \frac{a}{b} - 1 && \text{by subtracting 1 from both sides} \\ &= \frac{a}{b} - \frac{b}{b} && \text{by substitution} \\ &= \frac{a-b}{b} && \text{by the rule for subtracting fractions with a common denominator.} \end{aligned}$$

Hence

$$\sqrt{2} = \frac{a-b}{3b} \qquad \text{by dividing both sides by 3.}$$

But $a - b$ and $3b$ are integers (since a and b are integers and differences and products of integers are integers), and $3b \neq 0$ by the zero product property. Hence $\sqrt{2}$ is a quotient of the two integers $a - b$ and $3b$ with $3b \neq 0$, and so $\sqrt{2}$ is rational (by definition of rational). This contradicts the fact that $\sqrt{2}$ is irrational. *[The contradiction shows that the supposition is false.]* Hence $1 + 3\sqrt{2}$ is irrational.

■

Are There Infinitely Many Prime Numbers?

You know that a prime number is a positive integer that cannot be factored as a product of two smaller positive integers. Is the set of all such numbers infinite, or is there a largest prime number? The answer was known to Euclid, and a proof that the set of all prime numbers is infinite appears in Book 9 of his *Elements of Geometry*.

Euclid's proof requires one additional fact we have not yet established: If a prime number divides an integer, then it does not divide the next successive integer.

Proposition 4.8.3

For any integer a and any prime number p, if $p \mid a$ then $p \nmid (a + 1)$.

Proof (by contradiction): Suppose not. That is, suppose there exist an integer a and a prime number p such that $p \mid a$ and $p \mid (a + 1)$. Then, by definition of divisibility, there exist integers r and s such that $a = pr$ and $a + 1 = ps$. It follows that

$$1 = (a + 1) - a = ps - pr = p(s - r),$$

and so (since $s - r$ is an integer) $p \mid 1$. But, by Theorem 4.4.2, the only integer divisors of 1 are 1 and -1, and $p > 1$ because p is prime. Thus $p \leq 1$ and $p > 1$, which is a contradiction. *[Hence the supposition is false, and the proposition is true.]*

The idea of Euclid's proof is this: Suppose the set of prime numbers were finite. Then you could take the product of all the prime numbers and add 1. By Theorem 4.4.4 this number must be divisible by some prime number. But by Proposition 4.8.3, this number is not divisible by any of the prime numbers in the set. Hence there must be a prime number that is not in the set of all prime numbers, which is impossible.

The following formal proof fills in the details of this outline.

Theorem 4.8.4 Infinitude of the Primes

The set of prime numbers is infinite.

Proof (by contradiction): Suppose not. That is, suppose the set of prime numbers is finite. *[We must deduce a contradiction.]* Then some prime number p is the largest of all the prime numbers, and hence we can list the prime numbers in ascending order:

$$2, 3, 5, 7, 11, \ldots, p.$$

Let N be the product of all the prime numbers plus 1:

$$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$$

Then $N > 1$, and so, by Theorem 4.4.4, N is divisible by some prime number q. Because q is prime, q must equal one of the prime numbers $2, 3, 5, 7, 11, \ldots, p$. Thus, by definition of divisibility, q divides $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$, and so, by Proposition 4.8.3, q does not divide $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$, which equals N. Hence N is divisible by q and N is not divisible by q, and we have reached a contradiction. *[Therefore, the supposition is false and the theorem is true.]*

The proof of Theorem 4.8.4 shows that if you form the product of all the prime numbers up to a certain point and add one, the result, N, is divisible by a prime not on the list. The proof does not show that N is itself prime. In exercise 30 at the end of the section you will find a value for N that is not prime, although it is divisible by a prime.

When to Use Indirect Proof

The examples in this section and Section 4.7 have not provided a definitive answer to the question of when to prove a statement directly and when to prove it indirectly. Many

theorems can be proved either way. Usually, however, when both types of proof are possible, indirect proof is clumsier than direct proof. In the absence of obvious clues suggesting indirect argument, try first to prove a statement directly. Then, if that does not succeed, look for a counterexample. If the search for a counterexample is unsuccessful, look for a proof by contradiction or contraposition.

The Royal Society

Ben Joseph Green
(born 1977)

Philippe Desmazes/AFP/Getty Images

Terence Chi-Shen Tao
(born 1975)

Peter Bohler/Redux

Yitang Zhang
(born 1955)

Science & Society Picture Library/SSPL/Getty Images

Marie-Sophie Germain
(1776–1831)

Open Questions in Number Theory

In this section we proved that there are infinitely many prime numbers. There is no known formula for obtaining primes, but a few formulas have been found to be more successful at producing them than other formulas. One such is due to Marin Mersenne, a French monk who lived from 1588 to 1648. *Mersenne primes* have the form $2^p - 1$, where p is prime. Not all numbers of this form are prime, but because Mersenne primes are easier to test for primality than are other numbers, most of the largest known prime numbers are Mersenne primes.

An interesting question is whether there are infinitely many Mersenne primes. As of the date of publication of this book, the answer is not known, but new mathematical discoveries are being made every day and by the time you read this someone may have discovered the answer. Another formula that seems to produce a relatively large number of prime numbers is due to Fermat. *Fermat primes* are prime numbers of the form $2^{2^n} + 1$, where n is a positive integer. Are there infinitely many Fermat primes? Again, as of now, no one knows. Similarly unknown are whether there are infinitely many primes of the form $n^2 + 1$, where n is a positive integer, and whether there is always a prime number between integers n^2 and $(n + 1)^2$.

Another famous open question involving primes is the *twin primes conjecture*, which states that there are infinitely many pairs of prime numbers of the form p and $p + 2$. As with other well-known problems in number theory, this conjecture has withstood computer testing up to extremely large numbers, and some progress has been made toward a proof. In 2004, Ben Green and Terence Tao showed that for any integer $m > 1$, there is a sequence of m equally spaced integers all of which are prime. In 2013 Yitang Zhang proved that there are infinitely many pairs of prime numbers that differ by no more than 70,000,000. This is a lot more than 2, but Zhang's was the first discovery of any fixed upper bound between infinitely many pairs of prime numbers. In 2014 a group of mathematicians working collaboratively showed that the bound could be reduced from 70,000,000 to 246; still more than 2 but giving hope that a proof of the twin primes conjecture may be attainable.

Related to the twin primes conjecture is a conjecture made by Sophie Germain, a French mathematician born in 1776, who made significant progress toward a proof of Fermat's Last Theorem. Germain conjectured that there are infinitely many prime number pairs of the form p and $2p + 1$. Initial values of p with this property are 2, 3, 5, 11, 23, 29, 41, and 53, and computer testing has verified the conjecture for many additional values. In fact, as of the writing of this book, the largest prime p for which $2p + 1$ is also known to be prime is $2618163402417 \times 2^{1290000} - 1$. This is a number with 388,341 decimal digits! But compared with infinity, any number, no matter how large, is less than a drop in the bucket.

In 1844, the Belgian mathematician Eugène Catalan conjectured that the only solutions to the equation $x^n - y^m = 1$, where x, y, n, and m are all integers greater than 1, is $3^2 - 2^3 = 1$. This conjecture was finally proved by Preda Milhăilescu in 2002.

In 1993, while trying to prove Fermat's Last Theorem, an amateur number theorist, Andrew Beal, became intrigued by the equation $x^m + y^n = z^k$, where no two of x, y, or z have any common factor other than ± 1. When diligent effort, first by hand and then by computer, failed to reveal any solutions, Beal conjectured that no solutions exist. His conjecture has become known as the *Beal conjecture*, and he has offered a prize of $100,000 to anyone who can either prove or disprove it.

These are just a few of a large number of open questions in number theory. Many people believe that mathematics is a fixed subject that changes very little from one century to the next. In fact, more mathematical questions are being raised and more results are being discovered now than ever before in history.

TEST YOURSELF

1. The ancient Greeks discovered that in a right triangle where both legs have length 1, the ratio of the length of the hypotenuse to the length of one of the legs is not equal to a ratio of _____.
2. One way to prove that $\sqrt{2}$ is an irrational number is to assume that $\sqrt{2} = m/n$ for some integers m and n that have no common factor greater than 1, use the lemma that says that if the square of an integer is even then _____, and eventually show that m and n _____.
3. One way to prove that there are infinitely many prime numbers is to assume that there is a largest prime number p, construct the number _____, and then show that this number has to be divisible by a prime number that is greater than _____.

EXERCISE SET 4.8

1. A calculator display shows that $\sqrt{2} = 1.414213562$. Because $1.414213562 = \frac{1414213562}{1000000000}$, this suggests that $\sqrt{2}$ is a rational number, which contradicts Theorem 4.8.1. Explain the discrepancy.
2. Example 4.3.1(h) illustrates a technique for showing that any repeating decimal number is rational. A calculator display shows the result of a certain calculation as 40.72727272727. Can you be sure that the result of the calculation is a rational number? Explain.
3. Could there be a rational number whose first trillion digits are the same as the first trillion digits of $\sqrt{2}$? Explain.
4. A calculator display shows that the result of a certain calculation is 0.2. Can you be sure that the result of the calculation is a rational number?
5. Let S be the statement: The cube root of every irrational number is irrational. This statement is true, but the following "proof" is incorrect. Explain the mistake.

   "**Proof (by contradiction):** Suppose not. Suppose the cube root of every irrational number is rational. But $2\sqrt{2}$ is irrational because it is a product of a rational and an irrational number, and the cube root of $2\sqrt{2}$ is $\sqrt{2}$, which is irrational. This is a contradiction, and hence it is not true that the cube root of every irrational number is rational. Thus the statement to be proved is true."

Determine which statements in 6–16 are true and which are false. Prove those that are true and disprove those that are false.

6. $6 - 7\sqrt{2}$ is irrational.
7. $3\sqrt{2} - 7$ is irrational.
8. $\sqrt{4}$ is irrational.
9. $\sqrt{2}/6$ is irrational.
10. The sum of any two irrational numbers is irrational.
11. The difference of any two irrational numbers is irrational.
12. The positive square root of a positive irrational number is irrational.
13. If r is any rational number and s is any irrational number, then r/s is irrational.
14. The sum of any two positive irrational numbers is irrational.
15. The product of two irrational numbers is irrational.

H 16. If an integer greater than 1 is a perfect square, then its cube root is irrational.

17. Consider the following sentence: If x is rational then $\sqrt{x}$ is irrational. Is this sentence always true, sometimes true and sometimes false, or always false? Justify your answer.
18. **a.** Prove that for every integer a, if a^3 is even then a is even.
    b. Prove that $\sqrt[3]{2}$ is irrational.

19. **a.** Use proof by contradiction to show that for any integer n, it is impossible for n to equal both $3q_1 + r_1$ and $3q_2 + r_2$, where q_1, q_2, r_1, and r_2 are integers, $0 \le r_1 < 3$, $0 \le r_2 < 3$, and $r_1 \ne r_2$.

b. Use proof by contradiction, the quotient-remainder theorem, division into cases, and the result of part (a) to prove that for every integer n, if n^2 is divisible by 3 then n is divisible by 3.

c. Prove that $\sqrt{3}$ is irrational.

20. Give an example to show that if d is not prime and n^2 is divisible by d, then n need not be divisible by d.

H 21. The quotient-remainder theorem says not only that there exist quotients and remainders but also that the quotient and remainder of a division are unique. Prove the uniqueness. That is, prove that if a and d are integers with $d > 0$ and if q_1, r_1, q_2, and r_2 are integers such that

$$a = dq_1 + r_1 \quad \text{where} \quad 0 \le r_1 < d$$

and

$$a = dq_2 + r_2 \quad \text{where} \quad 0 \le r_2 < d,$$

then

$$q_1 = q_2 \quad \text{and} \quad r_1 = r_2.$$

H 22. Prove that $\sqrt{5}$ is irrational.

H 23. Prove that for any integer a, $9 \nmid (a^2 - 3)$.

24. An alternative proof of the irrationality of $\sqrt{2}$ counts the number of 2's on the two sides of the equation $2n^2 = m^2$ and uses the unique factorization of integers theorem to deduce a contradiction. Write a proof that uses this approach.

25. Use the proof technique illustrated in exercise 24 to prove that if n is any positive integer that is not a perfect square, then $\sqrt{n}$ is irrational.

H 26. Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

*** 27.** Prove that $\log_5(2)$ is irrational. (*Hint:* Use the unique factorization of integers theorem.)

H 28. Let $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1$. What remainder is obtained when N is divided by 2? 3? 5? 7? Justify your answer.

H 29. Suppose a is an integer and p is a prime number such that $p \mid a$ and $p \mid (a + 3)$. What can you deduce about p? Why?

30. Let $p_1, p_2, p_3, \ldots$ be a list of all prime numbers in ascending order. Here is a table of the first six:

p_1	p_2	p_3	p_4	p_5	p_6
2	3	5	7	11	13

H a. Let $N_1 = p_1$, $N_2 = p_1 \cdot p_2$, $N_3 = p_1 \cdot p_2 \cdot p_3, \ldots,$ $N_6 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6$. Calculate N_1, N_2, N_3, N_4, N_5, and N_6.

b. For each $i = 1, 2, 3, 4, 5, 6$, find whether N_i is itself prime or just has a prime factor less than itself. (*Hint:* Use the test for primality from exercise 31 in Section 4.7 to determine your answers.)

For exercises 31 and 32, use the fact that for every integer n,

$$n! = n(n-1) \cdots 3 \cdot 2 \cdot 1.$$

31. An alternative proof of the infinitude of the prime numbers begins as follows:

Proof: Suppose there are only finitely many prime numbers. Then one is the largest. Call it p. Let $M = p! + 1$. We will show that there is a prime number q such that $q > p$. Complete this proof.

H* 32. Prove that for every integer n, if $n > 2$ then there is a prime number p such that $n < p < n!$.

H* 33. Prove that if $p_1, p_2, \ldots,$ and p_n are distinct prime numbers with $p_1 = 2$ and $n > 1$, then $p_1 p_2 \cdots p_n + 1$ can be written in the form $4k + 3$ for some integer k.

H 34. **a.** Fermat's last theorem says that for every integer $n > 2$, the equation $x^n + y^n = z^n$ has no positive integer solution (solution for which x, y, and z are positive integers). Prove the following: If for every prime number $p > 2$, $x^p + y^p = z^p$ has no positive integer solution, then for any integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has no positive integer solution.

b. Fermat proved that there are no integers x, y, and z such that $x^4 + y^4 = z^4$. Use this result to remove the restriction in part (a) that n not be a power of 2. That is, prove that if n is a power of 2 and $n > 4$, then $x^n + y^n = z^n$ has no positive integer solution.

For exercises 35–38 note that to show there is a unique object with a certain property, show that (1) there is an object with the property and (2) if objects *A* and *B* have the property, then *A* = *B*.

35. Prove that there exists a unique prime number of the form $n^2 - 1$, where n is an integer that is greater than or equal to 2.

36. Prove that there exists a unique prime number of the form $n^2 + 2n - 3$, where n is a positive integer.

37. Prove that there is at most one real number a with the property that $a + r = r$ for every real number r. (Such a number is called an *additive identity*.)

38. Prove that there is at most one real number b with the property that $br = r$ for every real number r. (Such a number is called a *multiplicative identity*.)

ANSWERS FOR TEST YOURSELF

1. two integers **2.** the integer is even; have a common factor greater than 1 **3.** $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p + 1$; p

4.9 Application: The Handshake Theorem

The most important things in those first few seconds [of a job interview] are, basically, a firm handshake and a smile, good eye contact and really paying attention. —Pat Schaumann

Consider the following curious problem: At a meeting attended by a group of people, four people shook hands with one other person, six people shook hands with two other people, two people shook hands with three other people, and the rest shook hands with four other people. No two people shook hands with each other more than once, and a total of 23 handshakes occurred. How many people attended the meeting?

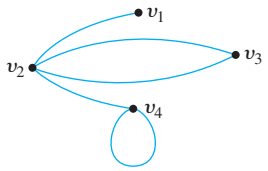
It turns out that a theorem about graphs helps to answer this question. Recall from Section 1.4 that if G is a graph and v is a vertex of G, then the degree of v, denoted $\deg(v)$, is the number of edges incident on v, with an edge that is a loop counted twice.

Definition

The total degree of a graph is the sum of the degrees of all the vertices of the graph.

Example 4.9.1 **The Total Degree of a Graph**

Find the degree of each vertex of the graph G shown below, and then find the total degree of the graph.



Solution

$\deg(v_1) = 1$; $\deg(v_2) = 4$; $\deg(v_3) = 2$; $\deg(v_4) = 3$
total degree of $G = 1 + 4 + 2 + 3 = 10$ ■

Note that in Example 4.9.1 the total degree of G, which is 10, equals twice the number of edges of G, which is 5. In fact, the total degree of *any* graph is twice the number of its edges. One way to see why this is so, at least for a graph without loops, is to imagine that the vertices of the graph represent people at a meeting and that each edge of the graph represents a handshake between two people. Each person participates in a certain number of handshakes—perhaps many, perhaps none—but if the numbers for each person are added together, a total is obtained, and, because each handshake is experienced by two different people, the total will equal twice the number of handshakes.

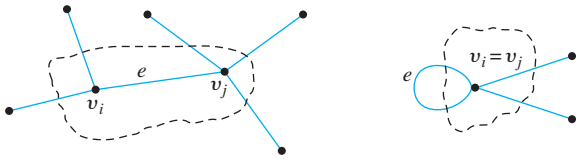
The handshake analogy is such an attractive way to understand the graph theory result that the theorem describing it is known as the *handshake theorem*. As the proof demonstrates, the conclusion is true even for a graph that contains loops.

Theorem 4.9.1 The Handshake Theorem

If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G. Specifically, if the vertices of G are $v_1, v_2, \ldots, v_n$, where n is a nonnegative integer, then

$$\begin{aligned}\text{the total degree of } G &= \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n)\\ &= 2 \cdot (\text{the number of edges of } G).\end{aligned}$$

Proof: Let G be a particular but arbitrarily chosen graph, and suppose that G has n vertices $v_1, v_2, \ldots, v_n$ and m edges, where n is a positive integer and m is a nonnegative integer. We claim that each edge of G contributes 2 to the total degree of G. For suppose e is an arbitrarily chosen edge with endpoints v_i and v_j. This edge contributes 1 to the degree of v_i and 1 to the degree of v_j. As shown below, this is true even if $i = j$, because an edge that is a loop is counted twice in computing the degree of the vertex on which it is incident.



$i \neq j$ $\qquad$ $i = j$

Therefore, e contributes 2 to the total degree of G. Since e was arbitrarily chosen, this shows that *each* edge of G contributes 2 to the total degree of G. Thus

$$\text{the total degree of } G = 2 \cdot (\text{the number of edges of } G).$$

The following corollary follows immediately from the handshake theorem.

Corollary 4.9.2

The total degree of a graph is even.

Proof: By Theorem 4.9.1 the total degree of G equals 2 times the number of edges of G, which is an integer, and so the total degree of G is even.

Example 4.9.2 **Determining Whether Certain Graphs Exist**

Draw a graph with the specified properties or show that no such graph exists.

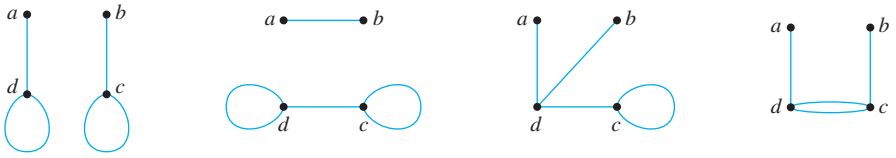
a. A graph with four vertices of degrees 1, 1, 2, and 3

b. A graph with four vertices of degree 1, 1, 3, and 3

Solution

a. No such graph exists. By Corollary 4.9.2 the total degree of a graph is even. But a graph with four vertices of degrees 1, 1, 2, and 3 would have a total degree of $1 + 1 + 2 + 3 = 7$, which is odd.

b. Let G be any of the graphs shown below.



In each case, no matter how the edges are labeled, $\deg(a) = 1$, $\deg(b) = 1$, $\deg(c) = 3$, and $\deg(d) = 3$. ■

Example 4.9.3 **Application to an Acquaintance Graph**

Is it possible in a group of nine people for each to be friends with exactly five others in the group?

Solution The answer is no. Imagine constructing an "acquaintance graph" in which each of the nine people is represented by a vertex and two vertices are joined by an edge if, and only if, the people they represent are friends. Suppose each of the people is friends with exactly five others. Then the degree of each of the nine vertices of the graph would be five, and so the total degree of the graph would be 45. But this contradicts Corollary 4.9.2, which says that the total degree of the graph is even. The contradiction shows that the supposition is false. Hence it is impossible for each person in a group of nine people to be friends with exactly five others in the group.

The following proposition can be deduced from Corollary 4.9.2 using properties of even and odd integers. ■

Proposition 4.9.3

In any graph there is an even number of vertices of odd degree.

Proof: Suppose G is any graph, and suppose G has n vertices of odd degree and m vertices of even degree, where n is a positive integer and m is a nonnegative integer. *[We must show that n is even.]* Let E be the sum of the degrees of all the vertices of even degree, O the sum of the degrees of all the vertices of odd degree, and T the total degree of G. If $u_1, u_2, \ldots, u_m$ are the vertices of even degree and $v_1, v_2, \ldots, v_n$ are the vertices of odd degree, then

$$\begin{aligned} E &= \deg(u_1) + \deg(u_2) + \cdots + \deg(u_m), \\ O &= \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n), \text{ and} \\ T &= \deg(u_1) + \cdots + \deg(u_m) + \deg(v_1) + \cdots + \deg(v_n) = E + O. \end{aligned}$$

Now T, the total degree of G, is an even integer by Corollary 4.9.2. Also E is even since either E is zero, which is even, or E is a sum of even numbers. Now since

$$T = E + O,$$

then

$$O = T - E.$$

Hence O is a difference of two even integers, and so O is even.

By assumption, $\deg(v_i)$ is odd for every integer $i = 1, 2, \ldots, n$. Thus O, an even integer, is a sum of the n odd integers $\deg(v_1), \deg(v_2), \ldots, \deg(v_n)$. But if a sum of n odd integers is even, then n is even. Therefore, n is even *[as was to be shown].*

Note In Section 5.4 you will have an opportunity to prove formally that any finite sum of even integers is even and that if a sum of n odd integers is even then n is even.

Example 4.9.4 **Applying the Fact That the Number of Vertices with Odd Degree Is Even**

Is there a graph with ten vertices of degrees 1, 1, 2, 2, 2, 3, 4, 4, 4, and 6?

Solution No. Such a graph would have three vertices of odd degree, which is impossible by Proposition 4.9.3.

Note that this same result could have been deduced directly from Corollary 4.9.2 by computing the total degree ($1+1+2+2+2+3+4+4+4+6 = 29$) and noting that it is odd. However, Proposition 4.9.3 gives the result without the need to perform this addition. ■

We can now show how to answer the question posed at the beginning of this section.

Example 4.9.5 **How Many People Attended the Meeting?**

At a meeting attended by a group of people, four people shook hands with one other person, six people shook hands with two other people, two people shook hands with three other people, and the rest shook hands with four other people. No two people shook hands with each other more than once, and a total of 23 handshakes occurred. How many people attended the meeting?

Solution Define a graph G by letting each vertex represent a person at the meeting and letting each edge represent one handshake between two people. Let x be the number of people who shook hands with four other people. Then

$$\text{the total degree of the graph} = 4\cdot 1 + 6\cdot 2 + 2\cdot 3 + x\cdot 4 = 22 + 4x$$

because 4 people shook hands with 1 other person, 6 people shook hands with 2 other people, 2 people shook hands with 3 other people, and x people shook hands with 4 other people. In addition, since a total of 23 handshakes occurred, the graph has 23 edges. By the handshake theorem (Theorem 4.9.1), the total degree is twice the number of edges. Hence

$$\text{the total degree of the graph} = 2\cdot 23 = 46.$$

It follows that

$$22 + 4x = 46.$$

Thus

$$4x = 46 - 22 = 24,$$

and so

$$x = \frac{24}{4} = 6.$$

In other words, six people at the meeting shook hands with four other people. Now the total number of people at the meeting is the sum of the number who shook hands with one other person, plus the number who shook hands with two other people, plus the number who shook hands with three other people, plus the number who shook hands with four other people. Therefore,

$$\text{the number of people at the meeting} = 4 + 6 + 2 + 6 = 18.$$ ■

Special Graphs

One important class of graphs consists of those that do not have any loops or parallel edges. Such graphs are called *simple*. In a simple graph, no two edges share the same set of endpoints, so specifying two endpoints is sufficient to determine an edge.

Definition and Notation

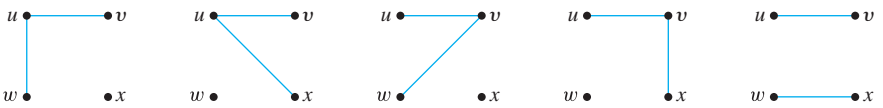
A **simple graph** is a graph that does not have any loops or parallel edges. In a simple graph, an edge with endpoints v and w is denoted $\{v, w\}$.

Example 4.9.6 **Some Simple Graphs**

Draw all simple graphs with the four vertices $\{u, v, w, x\}$ and two edges, one of which is $\{u, v\}$.

Solution

Since one edge of the graph is specified to be $\{u, v\}$, the possibilities for the other edge are $\{u, w\}$, $\{u, x\}$, $\{v, w\}$, $\{v, x\}$, and $\{w, x\}$. The resulting graphs are shown below.



Example 4.9.7 **Determining Whether Certain Simple Graphs Exist**

Draw a graph with the specified properties or show that no such graph exists.

a. A simple graph with six vertices and sixteen edges.

b. A simple graph with four vertices of degrees 1, 1, 3, and 3.

Solution

a. There is no simple graph with six vertices and sixteen edges.

Proof (by contradiction): Suppose there is a graph G with six vertices and sixteen edges. According to the handshake theorem (Theorem 4.9.1), since G has sixteen edges its total degree is $2 \cdot 16 = 32$, and because G has six vertices,

$$\text{the average degree of each vertex} = \frac{\text{the total degree}}{\text{the number of vertices}} = \frac{32}{6} = 5\frac{1}{3}.$$

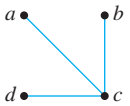
The only way this can happen is for at least one vertex—say v, to have degree greater than five. But since G has only six vertices, there are at most five other vertices to which v can be connected. Thus, in order for v to have degree greater than five, either there are at least two edges connecting v to one of the other vertices or there is a loop incident on v. In either case G would not be simple. Thus there is no simple graph that satisfies the given conditions.

b. There is no simple graph with four vertices of degrees 1, 1, 3, and 3.

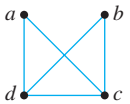
You might first try the same approach as in the solution for part (a): Assume such a graph exists and divide its total degree by the number of edges. Since the total degree

is $1 + 1 + 3 + 3 = 8$ and there are four vertices, the result is $8/4 = 2$. But this, by itself, is not a problem. You can easily find examples of simple graphs with four vertices where the average number of edges per vertex is two. Nonetheless, as the following argument shows, you will not be able to find a simple graph with total degree of eight and four vertices of degrees 1, 1, 3, and 3.

Proof (by contradiction): Suppose there is a simple graph G with four vertices of degrees 1, 1, 3, and 3. Call a and b the vertices of degree 1, and call c and d the vertices of degree 3. Since $\deg(c) = 3$ and G does not have any loops or parallel edges (because it is simple), there must be edges that connect c to a, b, and d.



By the same reasoning, there must be edges connecting d to a, b, and c.



But then $\deg(a) \geq 2$ and $\deg(b) \geq 2$, which contradicts the supposition that these vertices have degree 1. Hence the supposition is false, and consequently there is no simple graph with four vertices of degrees 1, 1, 3, and 3. ■

Another important class of graphs consists of those that are "complete" in the sense that each vertex in the graph is connected by exactly one edge to each other vertex in the graph.

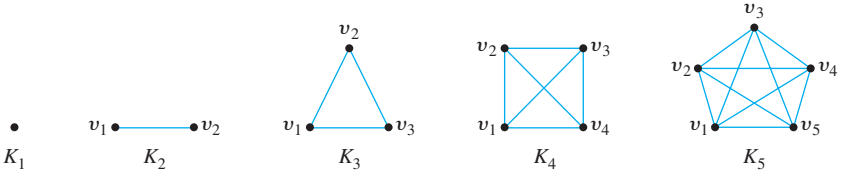
Note The K stands for the German word *komplett*, which means "complete."

Definition

Let n be a positive integer. A **complete graph on n vertices**, denoted K_n, is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.

Example 4.9.8 **Complete Graphs on n Vertices: K_1, K_2, K_3, K_4, K_5**

The complete graphs K_1, K_2, K_3, K_4, and K_5 can be drawn as follows:



■

Example 4.9.9 **The Number of Edges of K_n**

Prove that for any positive integer n, a complete graph on n vertices has $\frac{n(n-1)}{2}$ edges.

Solution

Proof: Suppose n is a positive integer and K_n is a complete graph on n vertices. Because each vertex of K_n is connected by exactly one edge to each of the other $n-1$ vertices of K_n, the degree of each vertex of K_n is $n-1$. Thus

$$\text{the total degree of } K_n = \begin{pmatrix}\text{the number of}\\ \text{vertices of } K_n\end{pmatrix} \cdot \begin{pmatrix}\text{the degree of}\\ \text{each vertex of } K_n\end{pmatrix} = n(n-1).$$

By the handshake theorem (Theorem 4.9.1), the total degree of K_n equals twice the number of its edges. So since the total degree is $n(n-1)$,

$$n(n-1) = 2 \cdot (\text{the number of edges of } K_n)$$

Dividing by 2 gives that

$$\text{the number of edges of } K_n = \frac{n(n-1)}{2}.$$ ■

In another class of graphs, called *complete bipartite graphs*, the vertex set can be separated into two subsets so that each vertex in one of the subsets is connected by exactly one edge to each vertex in the other subset but no vertex is connected by an edge to any other vertex in its own subset.

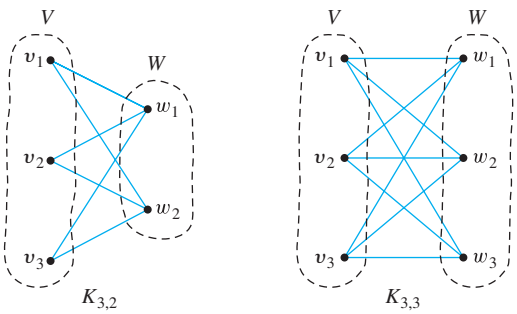
Definition

Let m and n be positive integers. A **complete bipartite graph on** (m, n) **vertices**, denoted $K_{m,n}$, is a simple graph whose vertices are divided into two distinct subsets, V with m vertices and W with n vertices, in such a way that

1. every vertex of $K_{m,n}$ belongs to one of V or W, but no vertex belongs to both V and W;
2. there is exactly one edge from each vertex of V to each vertex of W;
3. there is no edge from any one vertex of V to any other vertex of V;
4. there is no edge from any one vertex of W to any other vertex of W.

Example 4.9.10 **Complete Bipartite Graphs: $K_{3,2}$ and $K_{3,3}$**

The complete bipartite graphs $K_{3,2}$ and $K_{3,3}$ are illustrated below.



■

In exercise 23, you are asked to find the number of edges of $K_{m,n}$, where m and n are any positive integers.

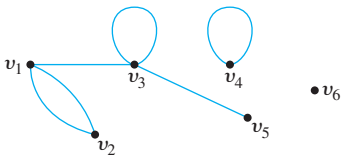
TEST YOURSELF

1. The total degree of a graph is defined as _____.
2. The handshake theorem says that the total degree of a graph is _____.
3. In any graph the number of vertices of odd degree is _____.
4. A simple graph is _____.
5. A complete graph on n vertices is a _____.
6. A complete bipartite graph on (m, n) vertices is a simple graph whose vertices can be divided into two distinct, non-overlapping sets, say V with m vertices and W with m vertices, in such a way that (1) there is _____ from each vertex of V to each vertex of W, (2) there is _____ from any one vertex of V to any other of V, and (3) there is _____ from any one vertex of W to any other vertex of W.

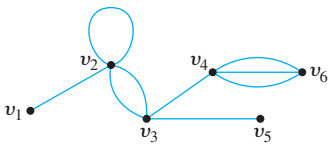
EXERCISE SET 4.9

In 1 and 2 find the degree of each vertex and the total degree of the graph. Check that the number of edges equals one-half of the total degree.

1.



2.



3. A graph has vertices of degrees 0, 2, 2, 3, and 9. How many edges does the graph have?
4. A graph has vertices of degrees 1, 1, 4, 4, and 6. How many edges does the graph have?

In each of 5–13 either draw a graph with the specified properties or explain why no such graph exists.

5. Graph with five vertices of degrees 1, 2, 3, 3, and 5.
6. Graph with four vertices of degrees 1, 2, 3, and 3.
7. Graph with four vertices of degrees 1, 1, 1, and 4.
8. Graph with four vertices of degrees 1, 2, 3, and 4.
9. Simple graph with four vertices of degrees 1, 2, 3, and 4.
10. Simple graph with five vertices of degrees 2, 3, 3, 3, and 5.
11. Simple graph with five vertices of degrees 1, 1, 1, 2, and 3.
12. Simple graph with six edges and all vertices of degree 3.
13. Simple graph with nine edges and all vertices of degree 3.
14. At a party attended by a group of people, two people knew one other person before the party, and five people knew two other people before the party. The rest of the people knew three other people before the party. A total of 15 pairs of people knew each other before the party.
    a. How many people attending the party knew three other people before the party?
    b. How many people attended the party?
15. A small social network contains three people who are network friends with six other people in the network, one person who is network friend with five other people in the network, and five people who are network friends with four other people in the network. The rest are network friends with three other people in the network. The network contains 41 pairs of network friends.
    a. How many people are network friends with three other people in the network?
    b. How many people are in the network?
16. a. In a group of 15 people, is it possible for each person to have exactly 3 friends? Justify your answer. (Assume that friendship is a symmetric relationship: If x is a friend of y, then y is a friend of x.)
    b. In a group of 4 people, is it possible for each person to have exactly 3 friends? Justify your answer.

17. In a group of 25 people, is it possible for each to shake hands with exactly 3 other people? Justify your answer.

18. Is there a simple graph, each of whose vertices has even degree? Justify your answer.

H 19. Suppose that G is a graph with v vertices and e edges and that the degree of each vertex is at least $d_{\min}$ and at most $d_{\max}$. Show that

$$\frac{1}{2}d_{\min} \cdot v \le e \le \frac{1}{2}d_{\max} \cdot v.$$

20. a. Draw K_6, a complete graph on six vertices.
b. Use the result of Example 4.9.9 to show that the number of edges of a simple graph with n vertices is less than or equal to $\frac{n(n-1)}{2}$.

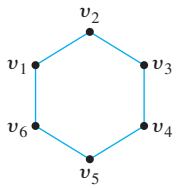
21. a. In a simple graph, must every vertex have degree that is less than the number of vertices in the graph? Why?
b. Can there be a simple graph that has four vertices all of different degrees? Why?
c. For any integer $n \ge 5$, can there be a simple graph that has n vertices all of different degrees? Why?

H 22. In a group of two or more people, must there always be at least two people who are acquainted with the same number of people within the group? Why?

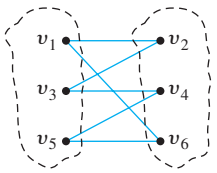
23. Recall that $K_{m,n}$ denotes a complete bipartite graph on (m, n) vertices.
a. Draw $K_{4,2}$.
b. Draw $K_{1,3}$.
c. Draw $K_{3,4}$.
d. How many vertices of $K_{m,n}$ have degree m? degree n?
e. What is the total degree of $K_{m,n}$?
f. Find a formula in terms of m and n for the number of edges of $K_{m,n}$. Justify your answer.

24. A (general) **bipartite graph** G is a simple graph whose vertex set can be partitioned into two disjoint nonempty subsets V_1 and V_2 such that vertices in V_1 may be connected to vertices in V_2, but no vertices in V_1 are connected to other vertices in V_1 and no vertices in V_2 are connected to other vertices in V_2. For example, the bipartite graph G illustrated in (i) can be redrawn as shown in (ii). From the drawing in (ii), you can see that G is bipartite with mutually disjoint vertex sets $V_1 = \{v_1, v_3, v_5\}$ and $V_2 = \{v_2, v_4, v_6\}$.

(i)

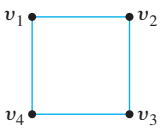


(ii)

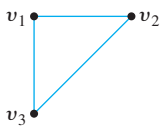


Find which of the following graphs are bipartite. Redraw the bipartite graphs so that their bipartite nature is evident.

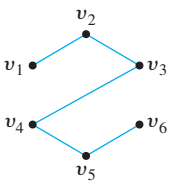
a.



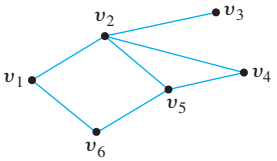
b.



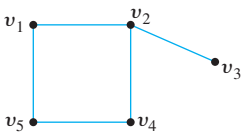
c.



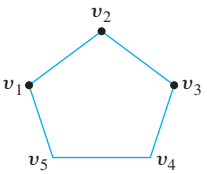
d.



e.



f.



25. Suppose r and s are any positive integers. Does there exist a graph G with the property that G has vertices of degrees r and s and of no other degrees? Explain.

ANSWERS FOR TEST YOURSELF

1. the sum of the degrees of all the vertices of the graph **2.** equal to the number of edges of the graph **3.** an even number **4.** a graph with no loops or parallel edges **5.** simple graph with n vertices whose set of edges contains exactly one edge for each pain of vertices **6.** one edge; no edge, no edge

4.10 Application: Algorithms

Begin at the beginning . . . and go on till you come to the end: then stop.
—Lewis Carroll, *Alice's Adventures in Wonderland*, 1865

Hulton Archive/Getty Images

Lady Lovelace
(1815–1852)

In this section we will show how the number theory facts developed in this chapter form the basis for some useful computer algorithms.

The word *algorithm* refers to a step-by-step method for performing some action. Some examples of algorithms in everyday life are food preparation recipes, directions for assembling equipment or hobby kits, sewing pattern instructions, and instructions for filling out income tax forms. Part of elementary school mathematics is devoted to learning algorithms for doing arithmetic such as multidigit addition and subtraction, multidigit (long) multiplication, and long division.

The idea of a computer algorithm is credited to Ada Augusta, Countess of Lovelace. Trained as a mathematician, she became very interested in Charles Babbage's design for an "Analytical Engine," a machine similar in concept to a modern computer. Lady Lovelace extended Babbage's explorations of how such a machine would operate, recognizing that its importance lay "in the possibility of using a given sequence of instructions repeatedly, the number of times being either preassigned or dependent on the results of the computation." This is the essence of a modern computer algorithm.

An Algorithmic Language

The algorithmic language used in this book is a kind of pseudocode, combining elements of Python, C, C^{++}, and Java, and ordinary, but fairly precise, English. We will use some of the formal constructs of computer languages—such as assignment statements, loops, and so forth—but we will ignore the more technical details, such as the requirement for explicit end-of-statement delimiters, the range of integer values available on a particular installation, and so forth. The algorithms presented in this text are intended to be precise enough to be easily translated into virtually any high-level computer language.

In high-level computer languages, the term **variable** is used to refer to a specific storage location in a computer's memory. To say that the variable x has the value 3 means that the memory location corresponding to x contains the number 3. A given storage location can hold only one value at a time. So if a variable is given a new value during program execution, then the old value is erased. The **data type** of a variable indicates the set in which the variable takes its values, whether the set of integers, or real numbers, or character strings, or the set $\{0, 1\}$ (for a Boolean variable), and so forth.

An **assignment statement** gives a value to a variable. It has the form

$$x := e,$$

where x is a variable and e is an expression. This is read "x is assigned the value e" or "let x be e." When an assignment statement is executed, the expression e is evaluated (using the current values of all the variables in the expression), and then its value is placed in the memory location corresponding to x (replacing any previous contents of this location).

Ordinarily, algorithm statements are executed one after another in the order in which they are written. **Conditional statements** allow this natural order to be overridden by using the current values of program variables to determine which algorithm statement will be executed next. Conditional statements are denoted either

a. **if** (*condition*) or b. **if** (*condition*) **then** s_1
then s_1
else s_2

where *condition* is a predicate involving algorithm variables and where s_1 and s_2 are algorithm statements or groups of algorithm statements. We generally use indentation to indicate that statements belong together as a unit. When ambiguity is possible, however, we may explicitly bind a group of statements together into a unit by preceding the group with the word **do** and following it with the words **end do**.

Execution of an **if-then-else** statement occurs as follows:

1. The *condition* is evaluated by substituting the current values of all algorithm variables appearing in it and evaluating the truth or falsity of the resulting statement.
2. If *condition* is true, then s_1 is executed and execution moves to the next algorithm statement following the **if-then-else** statement.
3. If *condition* is false, then s_2 is executed and execution moves to the next algorithm statement following the **if-then-else** statement.

Execution of an **if-then** statement is similar to execution of an **if-then-else** statement, except that if *condition* is false, execution passes immediately to the next algorithm statement following the **if-then** statement.

Often *condition* is called a **guard** because it is stationed before s_1 and s_2 and restricts access to them.

Example 4.10.1 **Execution of if-then-else and if-then Statements**

Consider the following algorithm segments:

a. **if** $x > 2$
then $y := x + 1$
else do $x := x - 1$
$y := 3 \cdot x$ **end do**

b. $y := 0$
if $x > 2$ **then** $y := 2^x$

What is the value of y after execution of these segments for the following values of x?
i. $x = 5$ ii. $x = 2$

Solution

a. (i) Because the value of x is 5 before execution, the guard condition $x > 2$ is true at the time it is evaluated. Hence the statement following **then** is executed, and so the value of $x + 1 = 5 + 1$ is computed and placed in the storage location corresponding to y. So after execution, $y = 6$.
(ii) Because the value of x is 2 before execution, the guard condition $x > 2$ is false at the time it is evaluated. Hence the statement following **else** is executed. The value of $x - 1 = 2 - 1$ is computed and placed in the storage location corresponding to x, and the value of $3 \cdot x = 3 \cdot 1$ is computed and placed in the storage location corresponding to y. So after execution, $y = 3$.

b. (i) Since $x = 5$ initially, the condition $x > 2$ is true at the time it is evaluated. So the statement following **then** is executed, and y obtains the value $2^5 = 32$.
(ii) Since $x = 2$ initially, the condition $x > 2$ is false at the time it is evaluated. Execution, therefore, moves to the next statement following the if-then statement, and the value of y does not change from its initial value of 0. ■

Iterative statements are used when a sequence of algorithm statements is to be executed over and over again. We will use two types of iterative statements: **while** loops and **for-next** loops.

A **while** loop has the form

while (*condition*)
[statements that make up the body of the loop]
end while

where *condition* is a predicate involving algorithm variables. The word **while** marks the beginning of the loop, and the words **end while** mark its end.

Execution of a **while** loop occurs as follows:

1. The *condition* is evaluated by substituting the current values of all the algorithm variables and evaluating the truth or falsity of the resulting statement.
2. If *condition* is true, all the statements in the body of the loop are executed in order. Then execution moves back to the beginning of the loop and the process repeats.
3. If *condition* is false, execution passes to the next algorithm statement following the loop.

The loop is said to be **iterated** (IT-a-rate-ed) each time the statements in the body of the loop are executed. Each execution of the body of the loop is called an **iteration** (it-er-AY-shun) of the loop.

Example 4.10.2 **Tracing Execution of a while Loop**

Trace the execution of the following algorithm segment by finding the values of all the algorithm variables each time they are changed during execution:

$i := 1, s := 0$
while $(i \leq 2)$
$s := s + i$
$i := i + 1$
end while

Solution Since i is given an initial value of 1, the condition $i \leq 2$ is true when the **while** loop is entered. So the statements within the loop are executed in order:

$$s = 0 + 1 = 1 \quad \text{and} \quad i = 1 + 1 = 2.$$

Then execution passes back to the beginning of the loop.

The condition $i \leq 2$ is evaluated using the current value of i, which is 2. The condition is true, and so the statements within the loop are executed again:

$$s = 1 + 2 = 3 \quad \text{and} \quad i = 2 + 1 = 3.$$

Then execution passes back to the beginning of the loop.

The condition $i \leq 2$ is evaluated using the current value of i, which is 3. This time the condition is false, and so execution passes beyond the loop to the next statement of the algorithm.

This discussion can be summarized in a table, called a **trace table**, that shows the current values of algorithm variables at various points during execution. The trace table for

a **while** loop generally gives all values immediately following each iteration of the loop. ("After the zeroth iteration" means the same as "before the first iteration.")

Trace Table

Variable Name	Iteration Number 0	1	2
i	1	2	3
s	0	1	3

■

The second form of iteration we will use is a **for-next** loop. A **for-next** loop has the following form:

for *variable* := *initial expression* **to** *final expression*
    [statements that make up
    the body of the loop]
next (*same*) *variable*

A **for-next** loop is executed as follows:

1. The **for-next** loop *variable* is set equal to the value of *initial expression*.
2. A check is made to determine whether the value of *variable* is less than or equal to the value of *final expression*.
3. If the value of *variable* is less than or equal to the value of *final expression*, then the statements in the body of the loop are executed in order, *variable* is increased by 1, and execution returns back to step 2.
4. If the value of *variable* is greater than the value of *final expression*, then execution passes to the next algorithm statement following the loop.

Example 4.10.3 **Trace Table for a for-next Loop**

Convert the **for-next** loop shown below into a **while** loop. Construct a trace table for the loop.

for $i := 1$ **to** 4
    $x := i^2$
next i

Solution The given **for-next** loop is equivalent to the following:

$i := 1$
while $(i \leq 4)$
    $x := i^2$
    $i := i + 1$
end while

Its trace table is as follows:

Trace Table

Variable Name	Iteration Number 0	1	2	3	4
x		1	4	9	16
i	1	2	3	4	5

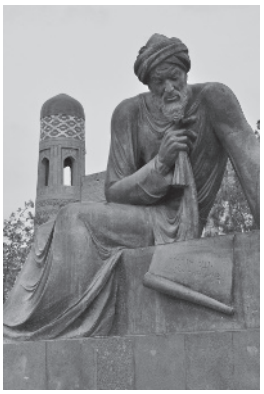
■

A Notation for Algorithms

Note Programming languages have various terms for subroutines: procedures, functions, routines, and subprograms.

We will express algorithms as subroutines that can be called upon by other algorithms as needed and used to transform a set of input variables with given values into a set of output variables with specific values. The output variables and their values are assumed to be returned to the calling algorithm. For example, the division algorithm specifies a procedure for taking any two positive integers as input and producing the quotient and remainder of the division of one number by the other as output. Whenever an algorithm requires such a computation, the algorithm can just "call" the division algorithm to do the job.

We generally include the following information when describing algorithms formally:



Eduard Kim/Shutterstock.com

al-Khowârizmî
(*ca. 780–850*)

1. The name of the algorithm, together with a list of input and output variables.
2. A brief description of how the algorithm works.
3. The input variable names, labeled by data type (whether integer, real number, and so forth).
4. The statements that make up the body of the algorithm, possibly with explanatory comments.
5. The output variable names, labeled by data type.

You may wonder where the word *algorithm* came from. It evolved from the last part of the name of the Persian mathematician Abu Ja'far Mohammed ibn Mûsâ al-Khowârizmî. During Europe's Dark Ages, the Arabic world enjoyed a period of intense intellectual activity. One of the great mathematical works of that period was a book written by al-Khowârizmî that contained foundational ideas for the subject of algebra. The translation of this book into Latin in the thirteenth century had a profound influence on the development of mathematics during the European Renaissance.

The Division Algorithm

For an integer a and a positive integer d, the quotient-remainder theorem guarantees the existence of integers q and r such that

$$a = dq + r \quad \text{and} \quad 0 \leq r < d.$$

In this section, we give an algorithm to calculate q and r for given a and d where a is nonnegative. (The extension to negative a is left to the exercises at the end of this section.) The following example illustrates the idea behind the algorithm. Consider trying to find the quotient and the remainder of the division of 32 by 9, but suppose that you do not remember your multiplication table and have to figure out the answer from basic

principles. The quotient represents that number of 9's that are contained in 32. The remainder is the number left over when all possible groups of 9 are subtracted. Thus you can calculate the quotient and remainder by repeatedly subtracting 9 from 32 until you obtain a number less than 9:

$$\begin{aligned} 32 - 9 &= 23 \geq 9, \text{ and} \\ 32 - 9 - 9 &= 14 \geq 9, \text{ and} \\ 32 - 9 - 9 - 9 &= 5 < 9. \end{aligned}$$

This shows that 3 groups of 9 can be subtracted from 32 with 5 left over. Thus the quotient is 3 and the remainder is 5.

Algorithm 4.10.1 Division Algorithm

[Given a nonnegative integer a and a positive integer d, the aim of the algorithm is to find integers q and r that satisfy the conditions $a = dq + r$ and $0 \leq r < d$. This is done by subtracting d repeatedly from a until the result is less than d but is still nonnegative.

$$0 \leq a - d - d - d - \cdots - d = a - dq < d.$$

The total number of d's that are subtracted is the quotient q. The quantity $a - dq$ equals the remainder r.]

Input: *a [a nonnegative integer], d [a positive integer]*

Algorithm Body:

$r := a, q := 0$
[Repeatedly subtract d from r until a number less than d is obtained. Add 1 to q each time d is subtracted.]
while $(r \geq d)$
    $r := r - d$
    $q := q + 1$
end while
[After execution of the **while** *loop, $a = dq + r$.]*

Output: *q, r [nonnegative integers]*

Note that the values of q and r obtained from the division algorithm are the same as those computed by the *div* and *mod* functions built into a number of computer languages. That is, if q and r are the quotient and remainder obtained from the division algorithm with input a and d, then the output variables q and r satisfy

$$q = a \text{ div } d \quad \text{and} \quad r = a \bmod d.$$

The next example asks for a trace table for the division algorithm.

Example 4.10.4 **Tracing the Division Algorithm**

Trace the action of Algorithm 4.10.1 on the input variables $a = 19$ and $d = 4$.

Solution Make a trace table as shown on the next page. The column under the kth iteration gives the states of the variables after the kth iteration of the loop.

Variable Name	Iteration Number 0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

The Euclidean Algorithm

The greatest common divisor of two integers a and b is the largest integer that divides both a and b. For example, the greatest common divisor of 12 and 30 is 6. The Euclidean algorithm provides a very efficient way to compute the greatest common divisor of two integers.

Definition

Let a and b be integers that are not both zero. The **greatest common divisor** of a and b, denoted $\mathbf{gcd}(a, b)$, is that integer d with the following properties:

1. d is a common divisor of both a and b. In other words,
$$d|a \quad \text{and} \quad d|b.$$
2. For every integer c, if c is a common divisor of both a and b, then c is less than or equal to d. In other words,
$$\text{for every integer } c, \text{ if } c|a \text{ and } c|b \text{ then } c \leq d.$$

Example 4.10.5 **Calculating Some gcd's**

a. Find gcd(72, 63).

b. Find gcd(10^{20}, 6^{30}).

c. In the definition of greatest common divisor, gcd(0, 0) is not allowed. Why not? What would gcd(0, 0) equal if it were found in the same way as the greatest common divisors for other pairs of numbers?

Solution

a. $72 = 9 \cdot 8$ and $63 = 9 \cdot 7$. So $9|72$ and $9|63$, and no integer larger than 9 divides both 72 and 63. Hence gcd(72, 63) = 9.

b. By the laws of exponents, $10^{20} = 2^{20} \cdot 5^{20}$ and $6^{30} = 2^{30} \cdot 3^{30} = 2^{20} \cdot 2^{10} \cdot 3^{30}$. It follows that
$$2^{20}|10^{20} \quad \text{and} \quad 2^{20}|6^{30},$$
and by the unique factorization of integers theorem, no integer larger than 2^{20} divides both 10^{20} and 6^{30} (because no more than twenty 2's divide 10^{20}, no 3's divide 10^{20}, and no 5's divide 6^{30}). Hence gcd(10^{20}, 6^{30}) = 2^{20}.

c. Suppose gcd(0, 0) were defined to be the largest common factor that divides 0 and 0. The problem is that *every* positive integer divides 0 and there is no largest integer. So there is no largest common divisor!

Calculating gcd's using the approach illustrated in Example 4.10.5 works only when the numbers can be factored completely. By the unique factorization of integers theorem, all numbers can, in principle, be factored completely. But, in practice, even using the highest-speed computers, the process is unfeasibly long for very large integers. Over 2,000 years ago, Euclid devised a method for finding greatest common divisors that is easy to use and is much more efficient than either factoring the numbers or repeatedly testing both numbers for divisibility by successively larger integers.

The Euclidean algorithm is based on the following two facts, which are stated as lemmas.

Lemma 4.10.1

If r is a positive integer, then $\gcd(r, 0) = r$.

Proof: Suppose r is a positive integer. *[We must show that the greatest common divisor of both r and 0 is r.]* Certainly, r is a common divisor of both r and 0 because r divides itself and also r divides 0 (since every positive integer divides 0). Also no integer larger than r can be a common divisor of r and 0 (since no integer larger than r can divide r). Hence r is the greatest common divisor of r and 0.

The proof of the second lemma is based on a clever pattern of argument that is used in many different areas of mathematics: To prove that $A = B$, prove that $A \leq B$ and that $B \leq A$.

Lemma 4.10.2

If a and b are any integers not both zero, and if q and r are any integers such that

$$a = bq + r,$$

then

$$\gcd(a, b) = \gcd(b, r).$$

Proof: *[The proof is divided into two sections: (1) proof that* $\gcd(a, b) \leq \gcd(b, r)$*, and (2) proof that* $\gcd(b, r) \leq \gcd(a, b)$*. Since each* gcd *is less than or equal to the other, the two must be equal.]*

1. **gcd(a, b) ≤ gcd(b, r):**
   a. *[We will first show that any common divisor of a and b is also a common divisor of b and r.]*

      Let a and b be integers, not both zero, and let c be a common divisor of a and b. Then $c \mid a$ and $c \mid b$, and so, by definition of divisibility, $a = nc$ and $b = mc$, for some integers n and m. Substitute into the equation

      $$a = bq + r$$

      to obtain

      $$nc = (mc)q + r.$$

(continued on page 252)

Then solve for r:

$$r = nc - (mc)q = (n - mq)c.$$

Now $n - mq$ is an integer, and so, by definition of divisibility, $c \mid r$. Because we already know that $c \mid b$, we can conclude that c is a common divisor of b and r *[as was to be shown].*

b. *[Next we show that* $\gcd(a, b) \leq \gcd(b, r)$*.]*

Now the greatest common divisor of a and b is defined because a and b are not both zero. Also, by part (a), every common divisor of a and b is a common divisor of b and r, and so the greatest common divisor of a and b is a common divisor of b and r. But then $\gcd(a, b)$ (being one of the common divisors of b and r) is less than or equal to the greatest common divisor of b and r:

$$\gcd(a, b) \leq \gcd(b, r).$$

2. **gcd(b, r) ≤ gcd(a, b):**
The second part of the proof is very similar to the first part. It is left as an exercise.

The Euclidean algorithm can be described as follows:

Euclidean Algorithm Description

1. Let A and B be integers with $A > B \geq 0$.
2. To find the greatest common divisor of A and B, first check whether $B = 0$. If it is, then $\gcd(A, B) = A$ by Lemma 4.10.1. If it isn't, then $B > 0$ and the quotient-remainder theorem can be used to divide A by B to obtain a quotient q and a remainder r:

$$A = Bq + r \quad \text{where } 0 \leq r < B.$$

By Lemma 4.10.2, $\gcd(A, B) = \gcd(B, r)$. Thus the problem of finding the greatest common divisor of A and B is reduced to the problem of finding the greatest common divisor of B and r.

[What makes this information useful is the fact that the larger number of the pair (B, r) is smaller than the larger number of the pair (A, B). The reason is that the value of r found by the quotient-remainder theorem satisfies

$$0 \leq r < B.$$

And, since by assumption $B < A$, we have that

$$0 \leq r < B < A.]$$

3. Now just repeat the process, starting again at (2), but use B instead of A and r instead of B. The repetitions are guaranteed to terminate eventually with $r = 0$ because each new remainder is less than the preceding one and all are nonnegative.

Note Strictly speaking, the fact that the repetitions eventually terminate is justified by the well-ordering principle for the integers, which is discussed in Section 5.4.

By the way, it is always the case that the number of steps required in the Euclidean algorithm is at most five times the number of digits in the smaller integer. This was proved by the French mathematician Gabriel Lamé (1795–1870).

The following example illustrates how to use the Euclidean algorithm.

Example 4.10.6 **Hand-Calculation of gcd's Using the Euclidean Algorithm**

Use the Euclidean algorithm to find gcd(330, 156).

Solution

1. Divide 330 by 156:

$$\begin{array}{r} 2 \quad \leftarrow \text{quotient} \\ 156\overline{)\ 330} \\ \underline{312} \\ 18 \quad \leftarrow \text{remainder} \end{array}$$

Thus $330 = 156 \cdot 2 + 18$, and hence gcd(330, 156) = gcd(156, 18) by Lemma 4.10.2.

2. Divide 156 by 18:

$$\begin{array}{r} 8 \quad \leftarrow \text{quotient} \\ 18\overline{)\ 156} \\ \underline{144} \\ 12 \quad \leftarrow \text{remainder} \end{array}$$

Thus $156 = 18 \cdot 8 + 12$, and hence gcd(156, 18) = gcd(18, 12) by Lemma 4.10.2.

3. Divide 18 by 12:

$$\begin{array}{r} 1 \quad \leftarrow \text{quotient} \\ 12\overline{)\ 18} \\ \underline{12} \\ 6 \quad \leftarrow \text{remainder} \end{array}$$

Thus $18 = 12 \cdot 1 + 6$, and hence gcd(18, 12) = gcd(12, 6) by Lemma 4.10.2.

4. Divide 12 by 6:

$$\begin{array}{r} 2 \quad \leftarrow \text{quotient} \\ 6\overline{)\ 12} \\ \underline{12} \\ 0 \quad \leftarrow \text{remainder} \end{array}$$

Thus $12 = 6 \cdot 2 + 0$, and hence gcd(12, 6) = gcd(6, 0) by Lemma 4.10.2.

Putting all the equations above together gives

$$\begin{aligned} \gcd(330, 156) &= \gcd(156, 18) \\ &= \gcd(18, 12) \\ &= \gcd(12, 6) \\ &= \gcd(6, 0) \\ &= 6 \qquad \text{by Lemma 4.10.1.} \end{aligned}$$

Therefore, gcd(330, 156) = 6. ■

The following is a version of the Euclidean algorithm written using formal algorithm notation.

Algorithm 4.10.2 Euclidean Algorithm

[Given two integers A and B with $A > B \geq 0$, this algorithm computes gcd(A, B)*. It is based on two facts:*

1. gcd(a, b) = gcd(b, r) *if a, b, q, and r are integers with $a = b \cdot q + r$ and $0 \leq r < b$.*
2. gcd$(a, 0) = a$*.]*

Input: *A, B [integers with $A > B \geq 0$]*

Algorithm Body:

$a := A$, $b := B$, $r := B$
[If $b \neq 0$, compute a mod b, the remainder of the integer division of a by b, and set r equal to this value. Then repeat the process using b in place of a and r in place of b.]
while $(b \neq 0)$
    $r := a \bmod b$
[The value of a mod b can be obtained by calling the division algorithm.]
    $a := b$
    $b := r$
end while
[After execution of the **while** *loop,* gcd$(A, B) = a$*.]*
gcd$:= a$

Output: gcd *[a positive integer]*

Example 4.10.7 **A Trace Table for the Euclidean Algorithm**

Construct a trace table for Algorithm 4.10.2 using $A = 330$ and $B = 156$, the same numbers as in Example 4.10.6.

Solution

A	330				
B	156				
a	330	156	18	12	6
b	156	18	12	6	0
r	156	18	12	6	0
gcd					6

■

TEST YOURSELF

1. When an algorithm statement of the form $x := e$ is executed, _____.
2. Consider an algorithm statement of the following form.

if (*condition*)
then s_1
else s_2

When such a statement is executed, the truth or falsity of the *condition* is evaluated. If *condition* is true, _____. If *condition* is false, _____.

3. Consider an algorithm statement of the following form.

   while (*condition*)
   [statements that make up the body of the loop]
   end while

   When such a statement is executed, the truth or falsity of the *condition* is evaluated. If *condition* is true, _____. If *condition* is false, _____.

4. Consider an algorithm statement of the following form.

   for *variable* : = *initial expression* **to** *final expression.*
   [statements that make up the body of the loop]
   next (*same*) *variable*

   When such a statement is executed, *variable* is set equal to the value of the *initial expression*, and a check is made to determine whether the value of *variable* is less than or equal to the value of *final expression*. If so, _____. If not, _____.

5. Given a nonnegative integer a and a positive integer d the division algorithm computes _____.

6. Given integers a and b, not both zero, gcd(a, b) is the integer d that satisfies the following two conditions: _____ and _____.

7. If r is a positive integer, then gcd(r, 0) = _____.

8. If a and b are integers not both zero and if q and r are nonnegative integers such that $a = bq + r$ then gcd(a, b) = _____.

9. Given positive integers A and B with $A > B$, the Euclidean algorithm computes _____.

EXERCISE SET 4.10

Find the value of z when each of the algorithm segments in 1 and 2 is executed.

1. $i := 2$
   if ($i > 3$ or $i \leq 0$)
   then $z := 1$
   else $z := 0$

2. $i := 3$
   if ($i \leq 3$ or $i > 6$)
   then $z := 2$
   else $z := 0$

3. Consider the following algorithm segment:
   if $x \cdot y > 0$ **then do** $y := 3 \cdot x$
   $x := x + 1$ **end do**
   $z := x \cdot y$
   Find the value of z if prior to execution x and y have the values given below.
   a. $x = 2, y = 3$
   b. $x = 1, y = 1$

Find the values of a and e after execution of the loops in 4 and 5 by first making trace tables for them.

4. $a := 2$
   for $i := 1$ **to** 3
   $a := 3a + 1$
   next i

5. $e := 2, f := 0$
   for $k := 1$ **to** 3
   $e := e \cdot k$
   $f := e + f$
   next k

Make a trace table to trace the action of Algorithm 4.10.1 for the input variables given in 6 and 7.

6. $a = 26, d = 7$

7. $a = 59, d = 13$

8. The following algorithm segment makes change; given an amount of money A between 1¢ and 99¢, it determines a breakdown of A into quarters (q), dimes (d), nickels (n), and pennies (p).

   $q := A \; div \; 25$
   $A := A \; mod \; 25$
   $d := A \; div \; 10$
   $A := A \; mod \; 10$
   $n := A \; div \; 5$
   $p := A \; mod \; 5$

   a. Trace this algorithm segment for $A = 69$.
   b. Trace this algorithm segment for $A = 87$.

Find the greatest common divisor of each of the pairs of integers in 9–12. (Use any method you wish.)

9. 27 and 72

10. 5 and 9

11. 7 and 21

12. 48 and 54

Use the Euclidean algorithm to hand-calculate the greatest common divisors of each of the pairs of integers in 13–16.

13. 1,188 and 385

14. 509 and 1,177

15. 832 and 10,933

16. 4,131 and 2,431

Make a trace table to trace the action of Algorithm 4.10.2 for the input variables given in 17–19.

17. 1,001 and 871

18. 5,859 and 1,232

19. 1,570 and 488

Definition: Integers a and b are said to be **relatively prime** if, and only if, their greatest common divisor is 1.

In 20 and 21 trace the action of Algorithm 4.10.2 to determine whether the integers are relatively prime.

20. 4,617 and 2,563 **21.** 34,391 and 6,728.

***H* 22.** Prove that for all positive integers a and b, $a|b$ if, and only if, $\gcd(a, b) = a$. (Note that to prove "A if, and only if, B," you need to prove "if A then B" and "if B then A.")

23. a. Prove that if a and b are integers, not both zero, and $d = \gcd(a, b)$, then a/d and b/d are integers with no common divisor that is greater than 1.

b. Write an algorithm that accepts the numerator and denominator of a fraction as input and produces as output the numerator and denominator of that fraction written in lowest terms. (The algorithm may call upon the Euclidean algorithm as needed.)

24. Complete the proof of Lemma 4.10.2 by proving the following: If a and b are any integers with $b \neq 0$ and q and r are any integers such that

$$a = bq + r.$$

then $\gcd(b, r) \leq \gcd(a, b)$.

***H* 25. a.** Prove: If a and d are positive integers and q and r are integers such that $a = dq + r$ and $0 < r < d$, then

$$-a = d(-(q + 1)) + (d - r)$$

and $0 < d - r < d$.

b. Indicate how to modify Algorithm 4.10.1 to allow for the input a to be negative.

26. a. Prove that if a, d, q, and r are integers such that $a = dq + r$ and $0 \leq r < d$, then

$$q = \lfloor a/d \rfloor \quad \text{and} \quad r = a - \lfloor a/d \rfloor \cdot d.$$

b. In a computer language with a built-in-floor function, *div* and *mod* can be calculated as follows:

$$a \text{ div } d = \lfloor a/d \rfloor \quad \text{and} \quad a \text{ mod } d = a - \lfloor a/d \rfloor \cdot d.$$

Rewrite the steps of Algorithm 4.10.2 for a computer language with a built-in floor function but without *div* and *mod*.

27. An alternative to the Euclidean algorithm uses subtraction rather than division to compute greatest common divisors. (After all, division is repeated subtraction.) It is based on the following lemma.

Lemma 4.10.3
If $a \geq b > 0$, then $\gcd(a, b) = \gcd(b, a - b)$.

Algorithm 4.10.3 Computing gcd's by Subtraction
[Given two positive integers A and B, variables a and b are set equal to A and B. Then a repetitive process begins. If $a \neq 0$, and $b \neq 0$, then the larger of a and b is set equal to $a - b$ (if $a \geq b$) or to $b - a$ (if $a < b$), and the smaller of a and b is left unchanged. This process is repeated over and over until eventually a or b becomes 0. By Lemma 4.10.3, after each repetition of the process,

$$\gcd(A, B) = \gcd(a, b).$$

After the last repetition,

$$\gcd(A, B) = \gcd(a, 0) \quad \textit{or} \quad \gcd(A, B) = \gcd(0, b)$$

depending on whether a or b is nonzero. But by Lemma 4.10.1,

$$\gcd(a, 0) = a \quad \textit{and} \quad \gcd(0, b) = b.$$

Hence, after the last repetition,

$$\gcd(A, B) = a \text{ if } a \neq 0 \quad \textit{or} \quad \gcd(A, B) = b \text{ if } b \neq 0.]$$

Input: A, B *[positive integers]*

Algorithm Body:
$a := A$, $b := B$
while ($a \neq 0$ and $b \neq 0$)
  if $a \geq b$ **then** $a := a - b$
    else $b := b - a$
end while
  if $a = 0$ **then** gcd $:= b$
  else gcd $:= a$
  [After execution of the **if-then-else** *statement,* gcd $= \gcd(A, B)$.*]*

Output: gcd *[a positive integer]*

a. Prove Lemma 4.10.3.

b. Trace the execution of Algorithm 4.10.3 for $A = 630$ and $B = 336$.

c. Trace the execution of Algorithm 4.10.3 for $A = 768$ and $B = 348$.

Exercises 28–32 refer to the following definition.

Definition: The **least common multiple** of two nonzero integers a and b, denoted **lcm(a, b)**, is the positive integer c such that
a. $a|c$ and $b|c$
b. for all positive integers m, if $a|m$ and $b|m$, then $c \leq m$.

28. Find
- **a.** lcm(12, 18)
- **b.** lcm($2^2 \cdot 3 \cdot 5$, $2^3 \cdot 3^2$)
- **c.** lcm(2800, 6125)

29. Prove that for all positive integers a and b, $\gcd(a, b) = \text{lcm}(a, b)$ if, and only if, $a = b$.

30. Prove that for all positive integers a and b, $a \mid b$ if, and only if, $\text{lcm}(a, b) = b$.

31. Prove that for all integers a and b, $\gcd(a, b) \mid \text{lcm}(a, b)$.

32. Prove that for all positive integers a and b, $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

ANSWERS FOR TEST YOURSELF

1. the expression e is evaluated (using the current values of all the variables in the expression), and this value is placed in the memory location corresponding to x (replacing any previous contents of the location) **2.** statement s_1 is executed; statement s_2 is executed **3.** all statements in the body of the loop are executed in order and then execution moves back to the beginning of the loop and the process repeats; execution passes to the next algorithm statement following the loop **4.** the statements in the body of the loop are executed in order, *variable* is increased by 1, and execution returns to the top of the loop; execution passes to the next algorithm statement following the loop **5.** integers q and r with the property that $n = dq + r$ and $0 \leq r < d$ **6.** d divides both a and b; if c is a common divisor of both a and b, then $c \leq d$ **7.** r **8.** $\gcd(b, r)$ **9.** the greatest common divisor of A and B (*Or*: $\gcd(A, B)$)

CHAPTER 5

SEQUENCES, MATHEMATICAL INDUCTION, AND RECURSION

One of the most important tasks of mathematics is to discover and characterize regular patterns, such as those associated with processes that are repeated. The main mathematical structure used in the study of repeated processes is the *sequence*, and the main mathematical tool used to verify conjectures about sequences is *mathematical induction*. In this chapter we introduce the notation and terminology of sequences, show how to use both ordinary and strong mathematical induction to prove properties about them, illustrate the various ways recursively defined sequences arise, describe a method for obtaining an explicit formula for a recursively defined sequence, and explain how to verify the correctness of such a formula. We also discuss a principle—the well-ordering principle for the integers—that is logically equivalent to the two forms of mathematical induction, and we show how to adapt mathematical induction to prove the correctness of computer algorithms. In the final section we discuss more general recursive definitions, including those for Boolean expressions and recursive functions, and we introduce a variation of mathematical induction, called structural induction, which is especially important in computer science.

5.1 Sequences

A mathematician, like a painter or poet, is a maker of patterns.
—G. H. Hardy, *A Mathematician's Apology*, 1940

Imagine that a person decides to count his ancestors. He has two parents, four grandparents, eight great-grandparents, and so forth. These numbers can be written in a row as

$$2, 4, 8, 16, 32, 64, 128, \ldots$$

Note The symbol ". . ." is called an *ellipsis*. It is shorthand for "and so forth."

To express the pattern of the numbers, suppose that each is labeled by an integer giving its position in the row.

Position in the row	1	2	3	4	5	6	7 . . .
Number of ancestors	2	4	8	16	32	64	128 . . .

Note Strictly speaking, the true value of A_k is less than 2^k when k is large, because ancestors from one branch of the family tree may also appear on other branches of the tree.

The number corresponding to position 1 is 2, which equals 2^1. The number corresponding to position 2 is 4, which equals 2^2. For positions 3, 4, 5, 6, and 7, the corresponding numbers are 8, 16, 32, 64, and 128, which equal 2^3, 2^4, 2^5, 2^6, and 2^7, respectively. For a general value of k, let A_k be the number of ancestors in the kth generation back. The pattern of computed values strongly suggests the following for each k:

$$A_k = 2^k.$$

Definition

A **sequence** is a function whose domain is either all the integers between two given integers or all the integers greater than or equal to a given integer.

We typically represent a sequence as a set of elements written in a row. In the sequence denoted

$$a_m, a_{m+1}, a_{m+2}, \ldots, a_n,$$

each individual element a_k (read "a sub k") is called a **term**. The k in a_k is called a **subscript** or **index**, m (which may be any integer) is the subscript of the **initial term**, and n (which must be an integer that is greater than or equal to m) is the subscript of the **final term**. The notation

$$a_m, a_{m+1}, a_{m+2}, \ldots$$

denotes an **infinite sequence**. An **explicit formula** or **general formula** for a sequence is a rule that shows how the values of a_k depend on k.

The following example shows that it is possible for two different formulas to give sequences with the same terms.

Example 5.1.1 **Finding Terms of Sequences Given by Explicit Formulas**

Define sequences $a_1, a_2, a_3, \ldots$ and $b_2, b_3, b_4, \ldots$ by the following explicit formulas:

$$a_k = \frac{k}{k+1} \quad \text{for every integer } k \geq 1,$$

$$b_i = \frac{i-1}{i} \quad \text{for every integer } i \geq 2.$$

Compute the first five terms of both sequences.

Solution

$$a_1 = \frac{1}{1+1} = \frac{1}{2} \qquad b_2 = \frac{2-1}{2} = \frac{1}{2}$$

$$a_2 = \frac{2}{2+1} = \frac{2}{3} \qquad b_3 = \frac{3-1}{3} = \frac{2}{3}$$

$$a_3 = \frac{3}{3+1} = \frac{3}{4} \qquad b_4 = \frac{4-1}{4} = \frac{3}{4}$$

$$a_4 = \frac{4}{4+1} = \frac{4}{5} \qquad b_5 = \frac{5-1}{5} = \frac{4}{5}$$

$$a_5 = \frac{5}{5+1} = \frac{5}{6} \qquad b_6 = \frac{6-1}{6} = \frac{5}{6}$$

As you can see, the first terms of both sequences are $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}$; in fact, it can be shown that all terms of both sequences are identical. ■

The next example shows that an infinite sequence may have a finite number of values.

Example 5.1.2 **An Alternating Sequence**

Compute the first six terms of the sequence $c_0, c_1, c_2, \ldots$ defined as follows:

$$c_j = (-1)^j \quad \text{for every integer } j \geq 0.$$

Solution

$$\begin{aligned} c_0 &= (-1)^0 = 1 \\ c_1 &= (-1)^1 = -1 \\ c_2 &= (-1)^2 = 1 \\ c_3 &= (-1)^3 = -1 \\ c_4 &= (-1)^4 = 1 \\ c_5 &= (-1)^5 = -1 \end{aligned}$$

Thus the first six terms are $1, -1, 1, -1, 1, -1$. By exercises 10 and 11 of Section 4.2, even powers of -1 equal 1 and odd powers of -1 equal -1. It follows that the sequence oscillates endlessly between 1 and -1. ■

In Examples 5.1.1 and 5.1.2 the task was to compute the first few terms of a sequence given by an explicit formula. The next example treats the question of how to find an explicit formula for a sequence with given initial terms. Any such formula is a guess, but it is useful to be able to make such guesses.

Example 5.1.3 **Finding an Explicit Formula to Fit Given Initial Terms**

Find an explicit formula for a sequence with the following initial terms:

$$1, \quad -\frac{1}{4}, \quad \frac{1}{9}, \quad -\frac{1}{16}, \quad \frac{1}{25}, \quad -\frac{1}{36}, \ldots.$$

Solution Denote the general term of the sequence by a_k and suppose the first term is a_1. Next observe that the denominator of each term is a perfect square. Thus the terms can be rewritten as

$$\begin{array}{cccccc} \frac{1}{1^2}, & \frac{(-1)}{2^2}, & \frac{1}{3^2}, & \frac{(-1)}{4^2}, & \frac{1}{5^2}, & \frac{(-1)}{6^2}. \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array}$$

Now note that the denominator of each term equals the square of the subscript of that term, and that the numerator equals ± 1. Hence

$$a_k = \frac{\pm 1}{k^2}.$$

Also the numerator oscillates back and forth between $+1$ and -1; it is $+1$ when k is odd and -1 when k is even. To achieve this oscillation, insert a factor of $(-1)^{k+1}$ (or $(-1)^{k-1}$) into the formula for a_k. *[For when k is odd, $k+1$ is even and thus $(-1)^{k+1} = +1$; and when k is even, $k+1$ is odd and thus $(-1)^{k+1} = -1$.]* Consequently, an explicit formula that gives the correct first six terms is

$$a_k = \frac{(-1)^{k+1}}{k^2} \quad \text{for every integer } k \geq 1.$$

Caution! It is also possible for two sequences to start off with the same initial values but diverge later on. See exercise 5 at the end of this section.

Note that making the first term a_0 would have led to the alternative formula

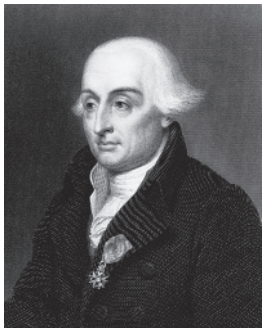
$$a_k = \frac{(-1)^k}{(k+1)^2} \quad \text{for every integer } k \geq 0.$$

You should check that this formula also gives the correct first six terms. ■

Summation Notation

Consider again the example in which $A_k = 2^k$ represents the number of ancestors a person has in the kth generation back. What is the total number of ancestors for the past six generations? The answer is

$$A_1 + A_2 + A_3 + A_4 + A_5 + A_6 = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 126.$$



Historical/Getty Images

Joseph Louis Lagrange (1736–1813)

It is convenient to use a shorthand notation to write such sums. In 1772 the French mathematician Joseph Louis Lagrange introduced the capital Greek letter sigma, Σ, to denote the word *sum* (or *summation*), and defined the summation notation as follows:

Definition

If m and n are integers and $m \leq n$, the symbol $\sum_{k=m}^{n} a_k$, read the **summation from *k* equals *m* to *n* of *a*-sub-*k***, is the sum of all the terms a_m, a_{m+1}, $a_{m+2}, \ldots, a_n$. We say that $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ is the **expanded form** of the sum, and we write

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

We call k the **index** of the summation, m the **lower limit** of the summation, and n the **upper limit** of the summation.

Example 5.1.4 **Computing Summations**

Let $a_1 = -2$, $a_2 = -1$, $a_3 = 0$, $a_4 = 1$, and $a_5 = 2$. Compute the following:

a. $\sum_{k=1}^{5} a_k$ b. $\sum_{k=2}^{2} a_k$ c. $\sum_{k=1}^{2} a_{2k}$

Solution

a. $\sum_{k=1}^{5} a_k = a_1 + a_2 + a_3 + a_4 + a_5 = (-2) + (-1) + 0 + 1 + 2 = 0$

b. $\sum_{k=2}^{2} a_k = a_2 = -1$

c. $\sum_{k=1}^{2} a_{2k} = a_{2\cdot 1} + a_{2\cdot 2} = a_2 + a_4 = -1 + 1 = 0$ ■

Oftentimes, the terms of a summation are expressed using an explicit formula. For instance, it is common to see summations such as

$$\sum_{k=1}^{5} k^2 \quad \text{or} \quad \sum_{i=0}^{8} \frac{(-1)^i}{i+1}.$$

Example 5.1.5 **When the Terms of a Summation Are Given by a Formula**

Compute $\sum_{k=1}^{5} k^2$.

Solution $$\sum_{k=1}^{5} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55.$$ ■

When the upper limit of a summation is a variable, an ellipsis is used to write the summation in expanded form.

Example 5.1.6 **Changing from Summation Notation to Expanded Form**

Write $\sum_{i=0}^{n} \frac{(-1)^i}{i+1}$ in expanded form:

Solution

$$\begin{aligned}\sum_{i=0}^{n} \frac{(-1)^i}{i+1} &= \frac{(-1)^0}{0+1} + \frac{(-1)^1}{1+1} + \frac{(-1)^2}{2+1} + \frac{(-1)^3}{3+1} + \cdots + \frac{(-1)^n}{n+1} \\ &= \frac{1}{1} + \frac{(-1)}{2} + \frac{1}{3} + \frac{(-1)}{4} + \cdots + \frac{(-1)^n}{n+1} \\ &= 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{(-1)^n}{n+1}\end{aligned}$$ ■

Example 5.1.7 **Changing from Expanded Form to Summation Notation**

Express the following using summation notation:

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n}.$$

Solution The general term of this summation can be expressed as $\frac{i+1}{n+i}$ for each integer i from 0 to n. Hence

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n} = \sum_{i=0}^{n} \frac{i+1}{n+i}.$$ ■

In Examples 5.1.6 and 5.1.7, the top index n of the summation is a *free variable* because it may be replaced by any integer greater than or equal to the bottom index, and each such replacement leads to a different summation. For any particular summation the top index acts like a constant. Thus when the top index also appears in the terms of the summation, as in Example 5.1.7, its value does not change from term to term. By contrast, the index variable in these examples is bound by the summation symbol. It must take every value from the bottom limit to the top limit in succession. The binding of an index variable in a summation is similar to the binding of a variable in a quantified statement or of a local variable in a computer program.

Writing a summation in expanded form helps relate it to our previous experience of working with sums. But for small values of n the expanded form may be misleading. For instance, consider trying to evaluate the following expression for $n = 1$:

$$1^2 + 2^2 + 3^2 + \cdots + n^2.$$

It may be tempting to write that when $n = 1$, $1^2 + 2^2 + 3^2 + \cdots + n^2$ equals

Caution!
Don't write this ⟶ $1^2 + 2^2 + 3^2 + \cdots + 1^2$. This is wrong!

The reason is that $1^2 + 2^2 + 3^2 + \cdots + n^2$ is simply a way of representing the sum of squares of consecutive integers starting with 1^2 and ending with n^2. Thus, when $n = 1$ the sum starts and ends with 1, and so it is just 1^2. If $n = 2$ the sum is $1^2 + 2^2$, and if $n = 3$ the sum is $1^2 + 2^2 + 3^2$.

Example 5.1.8 **Evaluating $a_1 + a_2 + a_3 + \cdots + a_n$ for Small n**

What is the value of $2^0 + 2^1 + 2^2 + \cdots + 2^n$ when $n = 0$, $n = 1$, and $n = 2$?

Solution When you evaluate a summation like $2^0 + 2^1 + 2^2 + \cdots + 2^n$ for small values of n, you can avoid a mistake by imagining it in summation notation. For instance,

$$2^0 + 2^1 + 2^2 + \cdots + 2^n = \sum_{i=0}^{n} 2^i.$$

So when $n = 0$, $2^0 + 2^1 + 2^2 + \cdots + 2^n$ has the value $\sum_{i=0}^{0} 2^i = 2^0 = 1$.

When $n = 1$, $2^0 + 2^1 + 2^2 + \cdots + 2^n$ has the value $\sum_{i=0}^{1} 2^i = 2^0 + 2^1 = 1 + 2$.

When $n = 2$, $2^0 + 2^1 + 2^2 + \cdots + 2^n$ has the value $\sum_{i=0}^{2} 2^i = 2^0 + 2^1 + 2^2 = 1 + 2 + 4$. ■

A more mathematically precise definition of summation, called a *recursive definition*, is the following:* If m is any integer, then

$$\sum_{k=m}^{m} a_k = a_m \quad \text{and} \quad \sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n \quad \text{for every integer } n > m.$$

When solving problems, it is often useful to rewrite a summation using the recursive form of the definition, either by grouping summands using a single summation sign or by separating off the final term of a summation.

Example 5.1.9 **Using a Single Summation Sign and Separating Off a Final Term**

a. Write $\sum_{k=0}^{n} 2^k + 2^{n+1}$ as a single summation.

b. Rewrite $\sum_{i=1}^{n+1} \frac{1}{i^2}$ by separating off the final term.

Solution

a. $\sum_{k=0}^{n} 2^k + 2^{k+1} = (2^0 + 2^1 + 2^2 + \cdots + 2^n) + 2^{n+1} = \sum_{k=0}^{n+1} 2^k$

b. $\sum_{i=1}^{n+1} \frac{1}{i^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} = \sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2}$ ■

In certain sums each term is a difference of two quantities. When you write such sums in expanded form, you sometimes see that all the terms cancel except the first and the last.

*Other recursively defined sequences are discussed later in this section and, in greater detail, in Section 5.6.

Example 5.1.10 **A Telescoping Sum**

Some sums can be transformed so that successive cancellation of terms collapses the final result like a telescope. For instance, observe that for every integer $k \geq 1$,

$$\frac{1}{k} - \frac{1}{k+1} = \frac{(k+1)-k}{k(k+1)} = \frac{1}{k(k+1)}.$$

Use this identity to find a simple expression for $\sum_{k=1}^{n} \frac{1}{k(k+1)}$.

Solution

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) \\ &= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n-1} - \frac{1}{n}\right) + \left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= 1 - \frac{1}{n+1}\end{aligned}$$

■

Product Notation

The notation for the product of a sequence of numbers is analogous to the notation for their sum. The Greek capital letter pi, Π, denotes a product. For example,

$$\prod_{k=1}^{5} a_k = a_1 a_2 a_3 a_4 a_5.$$

Definition

If m and n are integers and $m \leq n$, the symbol $\prod_{k=m}^{n} a_k$, read the **product from *k* equals *m* to *n* of *a*-sub-*k***, is the product of all the terms $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$.

We write

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdots a_n.$$

A recursive definition for the product notation is the following: If m is any integer, then

$$\prod_{k=m}^{m} a_k = a_m \quad \text{and} \quad \prod_{k=m}^{n} a_k = \left(\prod_{k=m}^{n-1} a_k\right) \cdot a_n \quad \text{for every integer } n > m.$$

Example 5.1.11 **Computing Products**

Compute the following products:

a. $\prod_{k=1}^{5} k$ b. $\prod_{k=1}^{1} \frac{k}{k+1}$

Solution

a. $\prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$ b. $\prod_{k=1}^{1} \frac{k}{k+1} = \frac{1}{1+1} = \frac{1}{2}$

■

Properties of Summations and Products

The following theorem states general properties of summations and products. The proof of the theorem is discussed in Section 5.6.

Theorem 5.1.1

If $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ are sequences of real numbers and c is any real number, then the following equations hold for any integer $n \geq m$:

1. $\displaystyle\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$
2. $\displaystyle c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$ generalized distributive law
3. $\displaystyle \left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} (a_k \cdot b_k).$

Example 5.1.12 **Using Properties of Summation and Product**

Let $a_k = k + 1$ and $b_k = k - 1$ for every integer k. Write each of the following expressions as a single summation or product:

a. $\displaystyle\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k$

b. $\displaystyle \left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right)$

Solution

a. $$\begin{aligned} \sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k &= \sum_{k=m}^{n} (k+1) + 2 \cdot \sum_{k=m}^{n} (k-1) && \text{by substitution} \\ &= \sum_{k=m}^{n} (k+1) + \sum_{k=m}^{n} 2 \cdot (k-1) && \text{by Theorem 5.1.1 (2)} \\ &= \sum_{k=m}^{n} ((k+1) + 2 \cdot (k-1)) && \text{by Theorem 5.1.1 (1)} \\ &= \sum_{k=m}^{n} (3k-1) && \text{by algebraic simplification} \end{aligned}$$

b. $$\begin{aligned} \left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) &= \left(\prod_{k=m}^{n} (k+1)\right) \cdot \left(\prod_{k=m}^{n} (k-1)\right) && \text{by substitution} \\ &= \prod_{k=m}^{n} ((k+1) \cdot (k-1)) && \text{by Theorem 5.1.1 (3)} \\ &= \prod_{k=m}^{n} (k^2 - 1) && \text{by algebraic simplification} \end{aligned}$$ ■

Change of Variable

Observe that $$\sum_{k=1}^{3} k^2 = 1^2 + 2^2 + 3^2$$

and also that $$\sum_{i=1}^{3} i^2 = 1^2 + 2^2 + 3^2.$$

Hence $$\sum_{k=1}^{3} k^2 = \sum_{i=1}^{3} i^2.$$

The symbol used to represent an index of a summation is an example of a local variable, often called a **dummy variable**, because, as illustrated above, it can be replaced by any other symbol as long as the replacement is made in each location where it occurs. Outside of that context (both before and after), the symbol may have another meaning entirely. In the same way, a symbol used to represent a variable in a universally or existentially quantified state can be replaced by any other symbol as long as the replacements are made consistently.

The appearance of a summation can be altered by more complicated changes of variable as well. For example, observe that

$$\begin{aligned}\sum_{j=2}^{4} (j-1)^2 &= (2-1)^2 + (3-1)^2 + (4-1)^2 \\ &= 1^2 + 2^2 + 3^2 \\ &= \sum_{k=1}^{3} k^2.\end{aligned}$$

A general procedure to transform the first summation into the second is illustrated in Example 5.1.13.

Example 5.1.13 **Transforming a Sum by a Change of Variable**

Transform the following summation by making the specified change of variable:

$$\textit{summation: } \sum_{k=0}^{6} \frac{1}{k+1} \qquad \textit{change of variable: } j = k+1$$

Solution First calculate the lower and upper limits of the new summation:

$$\begin{aligned}&\text{When } k = 0, \quad j = k+1 = 0+1 = 1.\\ &\text{When } k = 6, \quad j = k+1 = 6+1 = 7.\end{aligned}$$

Thus the new sum goes from $j = 1$ to $j = 7$.

Next calculate the general term of the new summation. You will need to replace each occurrence of k by an expression in j:

$$\begin{aligned}&\text{Since } j = k+1, \text{ then } k = j-1.\\ &\text{Hence } \frac{1}{k+1} = \frac{1}{(j-1)+1} = \frac{1}{j}.\end{aligned}$$

Finally, put the steps together to obtain

$$\sum_{k=0}^{6} \frac{1}{k+1} = \sum_{j=1}^{7} \frac{1}{j}. \qquad 5.1.1$$

■

Equation (5.1.1) can be transformed further by noting that because the j in the right-hand summation is a dummy variable, it may be replaced by any other variable name, as

long as the substitution is made in every location where j occurs. In particular, it is legal to substitute k in place of j to obtain

$$\sum_{j=1}^{7} \frac{1}{j} = \sum_{k=1}^{7} \frac{1}{k}. \tag{5.1.2}$$

Putting equations (5.1.1) and (5.1.2) together gives

$$\sum_{k=0}^{6} \frac{1}{k+1} = \sum_{k=1}^{7} \frac{1}{k}.$$

Sometimes it is necessary to shift the limits of one summation in order to add it to another. An example is the algebraic proof of the binomial theorem, given in Section 9.7. A general procedure for making such a shift when the upper limit is part of the summand is illustrated in the next example.

Example 5.1.14 **When the Upper Limit Appears in the Expression to Be Summed**

Rewrite the summation $\displaystyle\sum_{k=1}^{n+1}\left(\frac{k}{n+k}\right)$ so that the lower limit becomes 0 and the upper limit becomes n but the index of the summation remains k.

a. First, transform the summation by making the change of variable $j = k - 1$.

b. Second, transform the summation obtained in part (a) by changing all j's to k's.

Solution

a. The index variable k is bound by the summation symbol to take each of the values from 1 to $n + 1$ in succession.

When $k = 1$, then $j = 1 - 1 = 0$, and when $k = n + 1$, then $j = (n + 1) - 1 = n$. So the new lower limit is 0 and the new upper limit is n.

Now n is a constant with respect to the terms of the sum. Unlike k, its value does not change from one term to the next. In addition, since $j = k - 1$, then $k = j + 1$. Thus

$$\frac{k}{n+k} = \frac{j+1}{n+(j+1)}$$

and so the general term of the new summation is

$$\frac{j+1}{n+(j+1)}.$$

Therefore,

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{j=0}^{n} \frac{j+1}{n+(j+1)}. \tag{5.1.3}$$

b. Changing all the j's to k's in the right-hand side of equation (5.1.3) gives

$$\sum_{j=0}^{n} \frac{j+1}{n+(j+1)} = \sum_{k=0}^{n} \frac{k+1}{n+(k+1)}. \tag{5.1.4}$$

Combining equations (5.1.3) and (5.1.4) results in

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{k=0}^{n} \frac{k+1}{n+(k+1)}.$$

■

Factorial and "n Choose r" Notation

The product of all consecutive integers up to a given integer occurs so often in mathematics that it is given a special notation—*factorial* notation.

Definition

For each positive integer n, the quantity ***n* factorial** denoted ***n*!**, is defined to be the product of all the integers from 1 to n:

$$n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1.$$

Zero factorial, denoted 0!, is defined to be 1:

$$0! = 1.$$

The definition of zero factorial as 1 may seem odd, but, as you will see when you read Chapter 9, it is convenient for many mathematical formulas.

Example 5.1.15 **The First Ten Factorials**

$$\begin{aligned} 0! &= 1 & 1! &= 1 \\ 2! &= 2 \cdot 1 = 2 & 3! &= 3 \cdot 2 \cdot 1 = 6 \\ 4! &= 4 \cdot 3 \cdot 2 \cdot 1 = 24 & 5! &= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 \\ 6! &= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720 & 7! &= 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5{,}040 \\ 8! &= 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 & 9! &= 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 40{,}320 & &= 362{,}880 \end{aligned}$$

■

As you can see from the example above, the values of $n!$ grow very rapidly. For instance, $40! \cong 8.16 \times 10^{47}$, which is a number that is too large to be computed exactly using the standard integer arithmetic of the machine-specific implementations of many computer languages. (The symbol $\cong$ means "is approximately equal to.")

A recursive definition for factorial is the following: Given any nonnegative integer n,

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{if } n \geq 1. \end{cases}$$

Caution! Note that $n \cdot (n-1)!$ is to be interpreted as $n \cdot [(n-1)!]$.

The next example illustrates the usefulness of the recursive definition for making computations.

Example 5.1.16 **Computing with Factorials**

Simplify the following expressions:

a. $\dfrac{8!}{7!}$ b. $\dfrac{5!}{2! \cdot 3!}$ c. $\dfrac{1}{2! \cdot 4!} + \dfrac{1}{3! \cdot 3!}$ d. $\dfrac{(n+1)!}{n!}$ e. $\dfrac{n!}{(n-3)!}$

Solution

a. $\dfrac{8!}{7!} = \dfrac{8 \cdot 7!}{7!} = 8$

b. $\dfrac{5!}{2! \cdot 3!} = \dfrac{5 \cdot 4 \cdot 3!}{2! \cdot 3!} = \dfrac{5 \cdot 4}{2 \cdot 1} = 10$

c. $$\frac{1}{2!\cdot 4!}+\frac{1}{3!\cdot 3!}=\frac{1}{2!\cdot 4!}\cdot\frac{3}{3}+\frac{1}{3!\cdot 3!}\cdot\frac{4}{4}$$ by multiplying each numerator and denominator by just what is necessary to obtain a common denominator

$$=\frac{3}{3\cdot 2!\cdot 4!}+\frac{4}{3!\cdot 4\cdot 3!}$$ by rearranging factors

$$=\frac{3}{3!\cdot 4!}+\frac{4}{3!\cdot 4!}$$ because $3\cdot 2! = 3!$ and $4\cdot 3! = 4!$

$$=\frac{7}{144}$$ by the rule for adding fractions with a common denominator

d. $$\frac{(n+1)!}{n!}=\frac{(n+1)\cdot n!}{n!}=n+1$$

e. $$\frac{n!}{(n-3)!}=\frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)!}{(n-3)!}=n\cdot(n-1)\cdot(n-2)$$

$$=n^3-3n^2+2n$$ ■

An important use for the factorial notation is in calculating values of quantities, called *n choose r*, that occur in many branches of mathematics, especially those connected with the study of counting techniques and probability.

Definition

Let n and r be integers with $0 \le r \le n$. The symbol

$$\binom{n}{r}$$

is read "***n* choose *r***" and represents the number of subsets of size r that can be chosen from a set with n elements.

Observe that the definition implies that $\binom{n}{r}$ will always be an integer because it is a number of subsets. In Section 9.5 we will explore many uses of n choose r for solving problems involving counting, and we will prove the following computational formula:

Formula for Computing $\binom{n}{r}$

For all integers n and r with $0 \le r \le n$,

$$\binom{n}{r}=\frac{n!}{r!(n-r)!}.$$

In this chapter, we show how to compute its values. Because n choose r is always an integer, you can be sure that all the factors in the denominator of the formula will be canceled out by factors in the numerator. Many electronic calculators have keys for computing values of $\binom{n}{r}$. These are denoted in various ways such as nCr, $C(n, r)$, ${}^nC_r$, and $C_{n,r}$. The letter C is used because the quantities $\binom{n}{r}$ are also called *combinations*. Sometimes they are referred to as *binomial coefficients* because of the connection with the binomial theorem discussed in Section 9.7.

Example 5.1.17 **Computing $\binom{n}{r}$**

Use the formula for computing $\binom{n}{r}$ to evaluate the following expressions:

a. $\binom{8}{5}$ b. $\binom{4}{4}$ c. $\binom{n+1}{n}$

Solution

a. $$\binom{8}{5} = \frac{8!}{5!(8-5)!}$$

$$= \frac{8\cdot 7\cdot \cancel{6}\cdot \cancel{5}\cdot \cancel{4}\cdot \cancel{3}\cdot \cancel{2}\cdot 1}{(\cancel{5}\cdot \cancel{4}\cdot \cancel{3}\cdot \cancel{2}\cdot 1)\cdot(\cancel{3}\cdot \cancel{2}\cdot 1)}$$ always cancel common factors before multiplying

$$= 56.$$

b. $$\binom{4}{4} = \frac{4!}{4!(4-4)!} = \frac{4!}{4!0!} = \frac{\cancel{4\cdot 3\cdot 2\cdot 1}}{(\cancel{4\cdot 3\cdot 2\cdot 1})(1)} = 1$$

The fact that $0! = 1$ makes this formula computable. It gives the correct value because a set of size 4 has exactly one subset of size 4, namely itself.

c. $$\binom{n+1}{n} = \frac{(n+1)!}{n!((n+1)-n)!} = \frac{(n+1)!}{n!1!} = \frac{(n+1)\cdot \cancel{n!}}{\cancel{n!}} = n+1$$ ■

Sequences in Computer Programming

An important data type in computer programming consists of finite sequences. In computer programming contexts, these are usually referred to as *one-dimensional arrays*. For example, consider a program that analyzes the wages paid to a sample of 50 workers. Such a program might compute the average wage and the difference between each individual wage and the average. This would require that each wage be stored in memory for retrieval later in the calculation. To avoid the use of entirely separate variable names for all of the 50 wages, each is written as a term of a one-dimensional array:

$$\text{W[1], W[2], W[3], . . . , W[50].}$$

Note that the subscript labels are written inside square brackets. The reason is that until relatively recently, it was impossible to type actual dropped subscripts on most computer keyboards.

Example 5.1.18 **Dummy Variable in a Loop**

The index variable for a **for-next** loop is a local, or dummy, variable. For example, the following three algorithm segments all produce the same output:

1. **for** $i := 1$ **to** n
   print $a[i]$
   next i

2. **for** $j := 0$ **to** $n-1$
   print $a[j+1]$
   next j

3. **for** $k := 2$ **to** $n+1$
   print $a[k-1]$
   next k

■

The recursive definitions for summation, product, and factorial lead naturally to computational algorithms. For instance, here are two sets of pseudocode to find the sum of $a[1]$, $a[2], \ldots, a[n]$. The one on the left exactly mimics the recursive definition by initializing

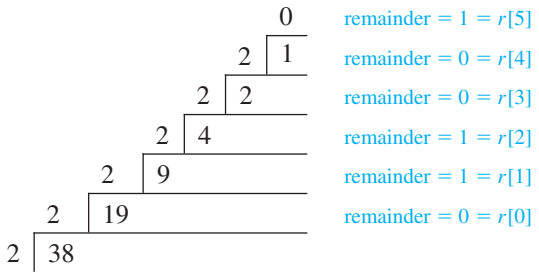
the sum to equal $a[1]$; the one on the right initializes the sum to equal 0. In both cases the output is $\sum_{k=1}^{n} a[k]$.

```
s := a[1]                    s := 0
for k := 2 to n              for k := 1 to n
    s := s + a[k]                s := s + a[k]
next k                       next k
```

Application: Algorithm to Convert from Base 10 to Base 2 Using Repeated Division by 2

Section 2.5 contains some examples of converting integers from decimal to binary notation. The method shown there, however, is only convenient to use with small numbers. A systematic algorithm to convert any nonnegative integer to binary notation uses repeated division by 2.

Suppose a is a nonnegative integer. Divide a by 2 using the quotient-remainder theorem to obtain a quotient $q[0]$ and a remainder $r[0]$. If the quotient is nonzero, divide by 2 again to obtain a quotient $q[1]$ and a remainder $r[1]$. Continue this process until a quotient of 0 is obtained. At each stage, the remainder must be less than the divisor, which is 2. Thus each remainder is always either 0 or 1. The process is illustrated below for $a = 38$. (Read the divisions from the bottom up.)



The results of all these divisions can be written as a sequence of equations:

$$\begin{aligned} 38 &= 19\cdot 2 + 0, \\ 19 &= 9\cdot 2 + 1, \\ 9 &= 4\cdot 2 + 1, \\ 4 &= 2\cdot 2 + 0, \\ 2 &= 1\cdot 2 + 0, \\ 1 &= 0\cdot 2 + 1. \end{aligned}$$

By repeated substitution, then

$$\begin{aligned} 38 &= 19\cdot 2 + 0 \\ &= (9\cdot 2 + 1)\cdot 2 + 0 = 9\cdot 2^2 + 1\cdot 2 + 0 \\ &= (4\cdot 2 + 1)\cdot 2^2 + 1\cdot 2 + 0 = 4\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0 \\ &= (2\cdot 2 + 0)\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0 \\ &= 2\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0 \\ &= (1\cdot 2 + 0)\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0 \\ &= 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0. \end{aligned}$$

Note that each coefficient of a power of 2 on the right-hand side of the previous page is one of the remainders obtained in the repeated division of 38 by 2. This is true for the left-most 1 as well, because $1 = 0 \cdot 2 + 1$. Thus

$$38_{10} = 100110_2 = (r[5]r[4]r[3]r[2]r[1]r[0])_2.$$

In general, if a nonnegative integer a is repeatedly divided by 2 until a quotient of zero is obtained and the remainders are found to be $r[0]$, $r[1], \ldots, r[k]$, then by the quotient-remainder theorem each $r[i]$ equals 0 or 1, and by repeated substitution from the theorem,

$$a = 2^k \cdot r[k] + 2^{k-1} \cdot r[k-1] + \cdots + 2^2 \cdot r[2] + 2^1 \cdot r[1] + 2^0 \cdot r[0]. \qquad 5.1.5$$

Thus the binary representation for a can be read from equation (5.1.5):

$$a_{10} = (r[k]r[k-1] \cdots r[2]r[1]r[0])_2.$$

Example 5.1.19 **Converting from Decimal to Binary Notation Using Repeated Division by 2**

Use repeated division by 2 to write the number 29_{10} in binary notation.

Solution

		0	remainder = $r[4] = 1$
	2	1	remainder = $r[3] = 1$
	2	3	remainder = $r[2] = 1$
	2	7	remainder = $r[1] = 0$
	2	14	remainder = $r[0] = 1$
2	29		

Hence $29_{10} = (r[4]r[3]r[2]r[1]r[0])_2 = 11101_2$. ■

The procedure we have described for converting from base 10 to base 2 is formalized in the following algorithm:

Algorithm 5.1.1 Decimal to Binary Conversion Using Repeated Division by 2

[In Algorithm 5.1.1 *the input is a nonnegative integer a. The aim of the algorithm is to produce a sequence of binary digits* r[0], r[1], r[2], . . . , r[k] *so that the binary representation of n is*

$$(r[k]r[k-1] \cdots r[2]r[1]r[0])_2.$$

That is,

$$a = 2^k \cdot r[k] + 2^{k-1} \cdot r[k-1] + \cdots + 2^2 \cdot r[2] + 2^1 \cdot r[1] + 2^0 \cdot r[0].]$$

Input: *a [a nonnegative integer]*

Algorithm Body:

$q := a, i := 0$

[Repeatedly perform the integer division of q by 2 *until q becomes* 0. *Store successive remainders in a one-dimensional array* r[0], r[1], r[2], . . . , r[k]. *Even if the initial-value of q equals* 0, *the loop should execute one time (so that* r[0] *is computed).*

Thus the guard condition for the **while** *loop is* $i = 0$ *or* $q \neq 0$.*]*

while ($i = 0$ *or* $q \neq 0$)
  $r[i] := q \bmod 2$
  $q := q \operatorname{div} 2$
  [$r[i]$ *and* q *can be obtained by calling the division algorithm.]*
  $i := i + 1$
end while

[After execution of this step, the values of $r[0], r[1], \ldots, r[i-1]$ *are all* 0*'s and* 1*'s, and* $a = (r[i-1]r[i-2]\cdots r[2]r[1]r[0])_2$.*]*

Output: $r[0], r[1], r[2], \ldots, r[i-1]$ *[a sequence of integers]*

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. The notation $\sum_{k=m}^{n} a_k$ is read "_____."
2. The expanded form of $\sum_{k=m}^{n} a_k$ is _____.
3. The value of $a_1 + a_2 + a_3 + \cdots + a_n$ when $n = 2$ is "_____."
4. The notation $\prod_{k=m}^{n} a_k$ is read "_____."
5. If n is a positive integer, then $n! =$ _____.
6. $\sum_{k=m}^{n} a_k + c\sum_{k=m}^{n} b_k =$ _____.
7. $\left(\prod_{k=m}^{n} a_k\right)\left(\prod_{k=m}^{n} b_k\right) =$ _____.

EXERCISE SET 5.1*

Write the first four terms of the sequences defined by the formulas in 1–6.

1. $a_k = \dfrac{k}{10+k}$, for every integer $k \geq 1$.
2. $b_j = \dfrac{5-j}{5+j}$, for every integer $j \geq 1$.
3. $c_i = \dfrac{(-1)^i}{3^i}$, for every integer $i \geq 0$.
4. $d_m = 1 + \left(\dfrac{1}{2}\right)^m$ for every integer $m \geq 0$.
5. $e_n = \left\lfloor \dfrac{n}{2} \right\rfloor \cdot 2$, for every integer $n \geq 0$.
6. $f_n = \left\lfloor \dfrac{n}{4} \right\rfloor \cdot 4$, for every integer $n \geq 1$.
7. Let $a_k = 2k + 1$ and $b_k = (k-1)^3 + k + 2$ for every integer $k \geq 0$. Show that the first three terms of these sequences are identical but that their fourth terms differ.

Compute the first fifteen terms of each of the sequences in 8 and 9, and describe the general behavior of these sequences in words. (A definition of logarithm is given in Section 7.1.)

8. $g_n = \lfloor \log_2 n \rfloor$ for every integer $n \geq 1$.
9. $h_n = n\lfloor \log_2 n \rfloor$ for every integer $n \geq 1$.

Find explicit formulas for sequences of the form $a_1, a_2, a_3, \ldots$ with the initial terms given in 10–16.

10. $-1, 1, -1, 1, -1, 1$
11. $0, 1, -2, 3, -4, 5$
12. $\dfrac{1}{4}, \dfrac{2}{9}, \dfrac{3}{16}, \dfrac{4}{25}, \dfrac{5}{36}, \dfrac{6}{49}$
13. $1 - \dfrac{1}{2}, \dfrac{1}{2} - \dfrac{1}{3}, \dfrac{1}{3} - \dfrac{1}{4}, \dfrac{1}{4} - \dfrac{1}{5}, \dfrac{1}{5} - \dfrac{1}{6}, \dfrac{1}{6} - \dfrac{1}{7}$
14. $\dfrac{1}{3}, \dfrac{4}{9}, \dfrac{9}{27}, \dfrac{16}{81}, \dfrac{25}{243}, \dfrac{36}{729}$
15. $0, -\dfrac{1}{2}, \dfrac{2}{3}, -\dfrac{3}{4}, \dfrac{4}{5}, -\dfrac{5}{6}, \dfrac{6}{7}$

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

16. 3, 6, 12, 24, 48, 96

*** 17.** Consider the sequence defined by $a_n = \dfrac{2n + (-1)^n - 1}{4}$ for every integer $n \geq 0$. Find an alternative explicit formula for a_n that uses the floor notation.

18. Let $a_0 = 2$, $a_1 = 3$, $a_2 = -2$, $a_3 = 1$, $a_4 = 0$, $a_5 = -1$, and $a_6 = -2$. Compute each of the summations and products below.

a. $\displaystyle\sum_{i=0}^{6} a_i$ **b.** $\displaystyle\sum_{i=0}^{0} a_i$ **c.** $\displaystyle\sum_{j=1}^{3} a_{2j}$ **d.** $\displaystyle\prod_{k=0}^{6} a_k$ **e.** $\displaystyle\prod_{k=2}^{2} a_k$

Compute the summations and products in 19–28.

19. $\displaystyle\sum_{k=1}^{5}(k+1)$ **20.** $\displaystyle\prod_{k=2}^{4} k^2$ **21.** $\displaystyle\sum_{k=1}^{3}(k^2+1)$

22. $\displaystyle\prod_{j=0}^{4}(-1)^j$ **23.** $\displaystyle\sum_{i=1}^{1} i(i+1)$ **24.** $\displaystyle\sum_{j=0}^{0}(j+1)\cdot 2^j$

25. $\displaystyle\prod_{k=2}^{2}\left(1-\frac{1}{k}\right)$ **26.** $\displaystyle\sum_{k=-1}^{1}(k^2+3)$

27. $\displaystyle\sum_{n=1}^{6}\left(\frac{1}{n}-\frac{1}{n+1}\right)$ **28.** $\displaystyle\prod_{i=2}^{5}\frac{i(i+2)}{(i-1)\cdot(i+1)}$

Write the summations in 29–32 in expanded form.

29. $\displaystyle\sum_{i=1}^{n}(-2)^i$ **30.** $\displaystyle\sum_{j=1}^{n} j(j+1)$ **31.** $\displaystyle\sum_{k=0}^{n+1}\frac{1}{k!}$ **32.** $\displaystyle\sum_{i=1}^{k+1} i(i!)$

Evaluate the summations and products in 33–36 for the indicated values of the variable.

33. $\dfrac{1}{1^2}+\dfrac{1}{2^2}+\dfrac{1}{3^2}+\cdots+\dfrac{1}{n^2}$; $n = 1$

34. $1(1!) + 2(2!) + 3(3!) + \cdots + m(m!)$; $m = 2$

35. $\left(\dfrac{1}{1+1}\right)\left(\dfrac{2}{2+1}\right)\left(\dfrac{3}{3+1}\right)\cdots\left(\dfrac{k}{k+1}\right)$; $k = 3$

36. $\left(\dfrac{1\cdot 2}{3\cdot 4}\right)\left(\dfrac{4\cdot 5}{6\cdot 7}\right)\left(\dfrac{6\cdot 7}{8\cdot 9}\right)\cdots\left(\dfrac{m\cdot(m+1)}{(m+2)\cdot(m+3)}\right)$; $m = 1$

Write each of 37–39 as a single summation.

37. $\displaystyle\sum_{i=1}^{k} i^3 + (k+1)^3$ **38.** $\displaystyle\sum_{k=1}^{m}\frac{k}{k+1}+\frac{m+1}{m+2}$

***H* 39.** $\displaystyle\sum_{m=0}^{n}(m+1)2^m + (n+2)2^{n+1}$

Rewrite 40–42 by separating off the final term.

40. $\displaystyle\sum_{i=1}^{k+1} i(i!)$ **41.** $\displaystyle\sum_{k=1}^{m+1} k^2$ **42.** $\displaystyle\sum_{m=1}^{n+1} m(m+1)$

Write each of 43–52 using summation or product notation.

43. $1^2 - 2^2 + 3^2 - 4^2 + 5^2 - 6^2 + 7^2$

44. $(1^3-1)-(2^3-1)+(3^3-1)-(4^3-1)+(5^3-1)$

45. $(2^2-1)\cdot(3^2-1)\cdot(4^2-1)$

46. $\dfrac{2}{3\cdot 4}-\dfrac{3}{4\cdot 5}+\dfrac{4}{5\cdot 6}-\dfrac{5}{6\cdot 7}+\dfrac{6}{7\cdot 8}$

47. $1 - r + r^2 - r^3 + r^4 - r^5$

48. $(1-t)\cdot(1-t^2)\cdot(1-t^3)\cdot(1-t^4)$

49. $1^3 + 2^3 + 3^3 + \cdots + n^3$

50. $\dfrac{1}{2!}+\dfrac{2}{3!}+\dfrac{3}{4!}+\cdots+\dfrac{n}{(n+1)!}$

51. $n + (n-1) + (n-2) + \cdots + 1$

52. $n+\dfrac{n-1}{2!}+\dfrac{n-2}{3!}+\dfrac{n-3}{4!}+\cdots+\dfrac{1}{n!}$

Transform each of 53 and 54 by making the change of variable $i = k + 1$.

53. $\displaystyle\sum_{k=0}^{5} k(k-1)$ **54.** $\displaystyle\prod_{k=1}^{n}\frac{k}{k^2+4}$

Transform each of 55–58 by making the change of variable $j = i - 1$.

55. $\displaystyle\sum_{i=1}^{n+1}\frac{(i-1)^2}{i\cdot n}$ **56.** $\displaystyle\sum_{i=3}^{n}\frac{i}{i+n-1}$

57. $\displaystyle\sum_{i=1}^{n-1}\frac{i}{(n-i)^2}$ **58.** $\displaystyle\prod_{i=n}^{2n}\frac{n-i+1}{n+i}$

Write each of 59–61 as a single summation or product.

59. $3\cdot\displaystyle\sum_{k=1}^{n}(2k-3)+\sum_{k=1}^{n}(4-5k)$

60. $2\cdot\displaystyle\sum_{k=1}^{n}(3k^2+4)+5\cdot\sum_{k=1}^{n}(2k^2-1)$

61. $\left(\displaystyle\prod_{k=1}^{n}\frac{k}{k+1}\right)\cdot\left(\prod_{k=1}^{n}\frac{k+1}{k+2}\right)$

Compute each of 62–76. Assume the values of the variables are restricted so that the expressions are defined.

62. $\dfrac{4!}{3!}$ **63.** $\dfrac{6!}{8!}$ **64.** $\dfrac{4!}{0!}$

65. $\dfrac{n!}{(n-1)!}$ **66.** $\dfrac{(n-1)!}{(n+1)!}$ **67.** $\dfrac{n!}{(n-2)!}$

68. $\dfrac{((n+1)!)^2}{(n!)^2}$ **69.** $\dfrac{n!}{(n-k)!}$ **70.** $\dfrac{n!}{(n-k+1)!}$

71. $\binom{5}{3}$ **72.** $\binom{7}{4}$ **73.** $\binom{3}{0}$

74. $\binom{5}{5}$ **75.** $\binom{n}{n-1}$ **76.** $\binom{n+1}{n-1}$

77. **a.** Prove that $n! + 2$ is divisible by 2, for every integer $n \geq 2$.

b. Prove that $n! + k$ is divisible by k, for every integer $n \geq 2$ and $k = 2, 3, \ldots, n$.

H **c.** Given any integer $m \geq 2$, is it possible to find a sequence of $m - 1$ consecutive positive integers none of which is prime? Explain your answer.

78. Prove that for all nonnegative integers n and r with $r + 1 \leq n$, $\binom{n}{r+1} = \dfrac{n-r}{r+1}\binom{n}{r}$.

79. Prove that if p is a prime number and r is an integer with $0 < r < p$, then $\binom{p}{r}$ is divisible by p.

80. Suppose $a[1], a[2], a[3], \ldots, a[m]$ is a one-dimensional array and consider the following algorithm segment:

```
sum := 0
for k := 1 to m
    sum := sum + a[k]
next k
```

Fill in the blanks below so that each algorithm segment performs the same job as the one shown in the exercise statement.

a.
```
sum := 0
for i := 0 to _____
    sum := _____
next i
```

b.
```
sum := 0
for j := 2 to _____
    sum := _____
next j
```

Use repeated division by 2 to convert (by hand) the integers in 81–83 from base 10 to base 2.

81. 90 **82.** 98 **83.** 205

Make a trace table to trace the action of Algorithm 5.1.1 on the input in 84–86.

84. 23 **85.** 28 **86.** 44

87. Write an informal description of an algorithm (using repeated division by 16) to convert a nonnegative integer from decimal notation to hexadecimal notation (base 16).

Use the algorithm you developed for exercise 87 to convert the integers in 88–90 to hexadecimal notation.

88. 287 **89.** 693 **90.** 2,301

91. Write a formal version of the algorithm you developed for exercise 87.

ANSWERS FOR TEST YOURSELF

1. the summation from k equals m to n of a-sub-k
2. $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ **3.** $a_1 + a_2$
4. the product from k equals m to n of a-sub-k
5. $n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$ (*Or:* $n \cdot (n-1)!$) **6.** $\displaystyle\sum_{k=m}^{n} (a_k + cb_k)$
7. $\displaystyle\prod_{k=m}^{n} a_k b_k$

5.2 Mathematical Induction I: Proving Formulas

A good proof is one which makes us wiser. —I. Manin, *A Course in Mathematical Logic*, 1977

In natural science courses, deduction and induction are presented as alternative modes of thought—deduction being to infer a conclusion from general principles using the laws of logical reasoning, and induction being to enunciate a general principle after observing it to hold in a large number of specific instances. Discovery of new mathematical facts often occurs through experimentation with examples, but *mathematical induction as a proof technique is not inductive but deductive*. Once proved by mathematical induction, a theorem is known just as certainly as if were proved by any other mathematical method. Thus,

in mathematics, inductive reasoning *is* used in the natural sciences sense, but only to make conjectures, not to prove them. For example, observe that

row 1	$1-\frac{1}{2}=\frac{1}{2}$
row 2	$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=\frac{1}{3}$
row 3	$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)=\frac{1}{4}$

This pattern seems so unlikely to occur by pure chance that it is reasonable to conjecture (though it is by no means certain) that the pattern holds true in general. To use mathematical induction to explore the conjecture, ask yourself: Is there something about the form of the pattern in one row that insures the pattern will be true in the next row? For instance, does the fact that the pattern is true in row 3 imply that it will also be true in a new row 4? To answer this question try substituting the right-hand side of the equation in row 3, namely $\frac{1}{4}$, into the expression $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right)$. That is,

$$\text{replace } \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right) \text{ by } \frac{1}{4} \text{ in } \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right).$$

When you do this, you obtain

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right)=\frac{1}{4}\left(1-\frac{1}{5}\right)=\frac{1}{4}\cdot\frac{4}{5}$$
$$=\frac{1}{5}.$$

So the pattern does extend to row 4! Does the process also work for going from row 1 to row 2? Yes! When you substitute the right-hand side of the equation in row 1, namely $\frac{1}{2}$, in place of $\left(1-\frac{1}{2}\right)$ in the left-hand side of the equation in row 2, the result is

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=\frac{1}{2}\left(1-\frac{1}{3}\right)$$
$$=\frac{1}{3}.$$

So the truth of the pattern in row 1 implies the truth of the pattern in row 2. Stop reading for a moment and use the same procedure to derive the truth of the pattern in row 3 from its truth in row 2 and then show that the same pattern extends to a new row 5. (This is exercise 1 at the end of this section.)

With this background you are ready to check out the general case. If you suppose that the pattern holds for an arbitrarily chosen row, can you show that the pattern holds for the next row? Suppose that k is any integer that is at least 2, and assume

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k}\right)=\frac{1}{k}.$$

Then

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k+1}\right)=\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{k+1}\right)$$
$$=\frac{1}{k}\left(1-\frac{1}{k+1}\right)=\frac{1}{k}\left(\frac{k+1}{k+1}-\frac{1}{k+1}\right)=\frac{1}{k}\left(\frac{k}{k+1}\right)=\frac{1}{k+1}.$$

Thus for any integer k greater than or equal to 2,

$$\text{if } \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k}\right)=\frac{1}{k} \quad \text{then} \quad \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k+1}\right)=\frac{1}{k+1}.$$

This example illustrates the basic idea of the principle of mathematical induction. It shows that as long as the pattern holds in one row, then it has to hold in the next larger row. But this implies that the pattern holds in *every* row no matter how far down the table it might be. The reason is that since the pattern holds in row 1, it holds in row 2. And since it holds in row 2, it holds in row 3. And since it holds in row 3, it holds in row 4. And since it holds in row 4, it holds in row 5. And so on, and so on, forever!

Principle of Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For every integer $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement

$$\text{for every integer } n \geq a, P(n)$$

is true.

The first known use of mathematical induction occurs in the work of the Italian scientist Francesco Maurolico in 1575. In 1653 Blaise Pascal gave a clear description of the technique, and in 1883 Augustus De Morgan (best known for De Morgan's laws) gave the process the name *mathematical induction*. An equivalent logical inference rule, now known as the *well-ordering principle* (see Section 5.4), was used implicitly by mathematicians in ancient Greece, in the middle ages by Campanus of Novara, and in the seventeenth century by Pierre de Fermat, who called it the "method of infinite descent."

To visualize the idea of mathematical induction, imagine an infinite collection of dominoes positioned one behind the other in such a way that if any given domino falls backward, it makes the one behind it fall backward also. (See Figure 5.2.1.) Then imagine that the first domino falls backward. What happens? . . . They all fall down!

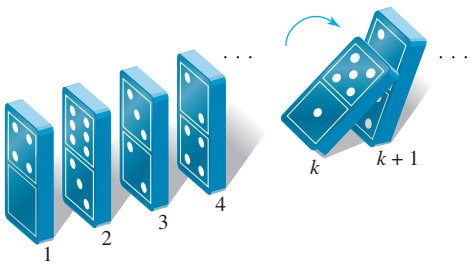


FIGURE 5.2.1 If the kth domino falls backward, it pushes the $(k+1)$st domino backward also.

To see the connection between this image and the principle of mathematical induction, let $P(n)$ be the sentence "The nth domino falls backward." It is given that for each $k \geq 1$, if $P(k)$ is true (the kth domino falls backward), then $P(k+1)$ is also true (the $(k+1)$st domino falls backward). It is also given that $P(1)$ is true (the first domino falls backward). Thus by

the principle of mathematical induction, $P(n)$ (the nth domino falls backward) is true for every integer $n \geq 1$.

The validity of proof by mathematical induction is generally taken as an axiom. That is why it is referred to as the *principle* of mathematical induction rather than as a theorem. It is equivalent to the following property of the integers, which is easy to accept on intuitive grounds:

> Suppose S is any set of integers satisfying (1) a is in S, and (2) for every integer $k \geq a$, if k is in S then $k + 1$ is in S. Then S contains every integer greater than or equal to a.

To understand the equivalence of this formulation and the one given earlier, let S be the set of all integers for which $P(n)$ is true.

Proving a statement by mathematical induction is a two-step process. The first step is called the *basis step*, and the second step is called the *inductive step*.

Method of Proof by Mathematical Induction

Consider a statement of the form, "For every integer $n \geq a$, a property $P(n)$ is true." To prove such a statement, perform the following two steps:

Step 1 (basis step): Show that $P(a)$ is true.

Step 2 (inductive step): Show that for every integer $k \geq a$, if $P(k)$ is true then $P(k + 1)$ is true. To perform this step,

suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.

[This supposition is called the **inductive hypothesis***.]*

Then

show that $P(k + 1)$ is true.

The following example shows how to use mathematical induction to prove a formula for the sum of the first n integers.

Example 5.2.1 **Sum of the First *n* Integers**

Use mathematical induction to prove that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for every integer } n \geq 1.$$

Solution To construct a proof by induction, you must first identify the property $P(n)$. In this case, $P(n)$ is the equation

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \quad \leftarrow \text{the property } (P(n))$$

Note The property is just the equation. The proof will show that the equation is true for every integer $n \geq 1$.

[To see that P(n) is a sentence, note that its subject is "the sum of the integers from 1 *to n" and its verb is "equals."]*

In the basis step of the proof, you must show that the property is true for $n = 1$, or, in other words, that $P(1)$ is true. Now $P(1)$ is obtained by substituting 1 in place of n in $P(n)$. The left-hand side of $P(1)$ is the sum of all the successive integers starting at 1 and ending at 1. This is just 1. Thus $P(1)$ is

$$1 = \frac{1(1+1)}{2}. \quad \leftarrow \text{basis } (P(1))$$

Note To write $P(1)$, just copy $P(n)$ and replace each n by 1.

Of course, this equation is true because the right-hand side is

$$\frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1,$$

which equals the left-hand side.

In the inductive step, you assume that $P(k)$ is true, for a particular but arbitrarily chosen integer k with $k \geq 1$. *[This assumption is the inductive hypothesis.]* You must then show that $P(k+1)$ is true. What are $P(k)$ and $P(k+1)$? $P(k)$ is obtained by substituting k for every n in $P(n)$. Thus $P(k)$ is

Note To write $P(k)$, just copy $P(n)$ and replace each n by k.

$$\boxed{1 + 2 + \cdots + k = \frac{k(k+1)}{2}.} \quad \leftarrow \text{inductive hypothesis } (P(k))$$

Similarly, $P(k+1)$ is obtained by substituting the quantity $(k+1)$ for every n that appears in $P(n)$. Thus $P(k+1)$ is

$$1 + 2 + \cdots + (k+1) = \frac{(k+1)((k+1)+1)}{2},$$

or, equivalently,

Note To write $P(k+1)$, just copy $P(n)$ and replace each n by $(k+1)$.

$$\boxed{1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}.} \quad \leftarrow \text{to show } (P(k+1))$$

Now the inductive hypothesis is the supposition that $P(k)$ is true. How can this supposition be used to show that $P(k+1)$ is true? $P(k+1)$ is an equation, and the truth of an equation can be shown in a variety of ways. One of the most straightforward is to use the inductive hypothesis along with algebra and other known facts to separately transform the left-hand and right-hand sides until you see that they are the same. In this case, the left-hand side of $P(k+1)$ is

$$1 + 2 + \cdots + (k+1),$$

which equals

$$(1 + 2 + \cdots + k) + (k+1)$$

The next-to-last term is k because the terms are successive integers and the last term is $k+1$.

By substitution from the inductive hypothesis,

$$\begin{aligned}
&(1 + 2 + \cdots + k) + (k+1) \\
&\quad = \frac{k(k+1)}{2} + (k+1) && \text{since the inductive hypothesis says that } 1 + 2 + \cdots + k = \tfrac{k(k+1)}{2} \\
&\quad = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} && \text{by multiplying the numerator and denominator of the second term by 2 to obtain a common denominator} \\
&\quad = \frac{k^2 + k}{2} + \frac{2k+2}{2} && \text{by multiplying out the two numerators} \\
&\quad = \frac{k^2 + 3k + 2}{2} && \text{by adding fractions with the same denominator and combining like terms.}
\end{aligned}$$

So the left-hand side of $P(k+1)$ is $\frac{k^2+3k+2}{2}$. Now the right-hand side of $P(k+1)$ is

$$\frac{(k+1)(k+2)}{2} = \frac{k^2 + 3k + 2}{2} \quad \text{by multiplying out the numerator.}$$

Thus the two sides of $P(k+1)$ are equal to each other, and so the equation $P(k+1)$ is true.

This discussion is summarized as follows:

Theorem 5.2.1 Sum of the First *n* Integers

For every integer $n \geq 1$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof (by mathematical induction): Let the property $P(n)$ be the equation

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}. \qquad \leftarrow P(n)$$

Show that P(1) is true:

To establish $P(1)$, we must show that

$$1 = \frac{1(1+1)}{2}. \qquad \leftarrow P(1)$$

But the left-hand side of this equation is 1 and the right-hand side is

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1$$

also. Hence $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k+1) is also true:

[Suppose that P(k) is true for a particular but arbitrarily chosen integer $k \geq 1$. That is:] Suppose that k is any integer with $k \geq 1$ such that

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}. \qquad \leftarrow P(k)$$

inductive hypothesis

[We must show that $P(k+1)$ is true. That is:] We must show that

$$1 + 2 + 3 + \cdots + (k+1) = \frac{(k+1)[(k+1)+1]}{2},$$

or, equivalently, that

$$1 + 2 + 3 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}. \qquad \leftarrow P(k+1)$$

[We will show that the left-hand side and the right-hand side of $P(k+1)$ are equal to the same quantity and thus are equal to each other.]

The left-hand side of $P(k+1)$ is

$$\begin{aligned}
&1 + 2 + 3 + \cdots + (k+1) \\
&\quad = 1 + 2 + 3 + \cdots + k + (k+1) && \text{by making the next-to-last term explicit} \\
&\quad = \frac{k(k+1)}{2} + (k+1) && \text{by substitution from the inductive hypothesis} \\
&\quad = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&\quad = \frac{k^2 + k}{2} + \frac{2k+2}{2} \\
&\quad = \frac{k^2 + 3k + 2}{2} && \text{by algebra.}
\end{aligned}$$

And the right-hand side of $P(k+1)$ is

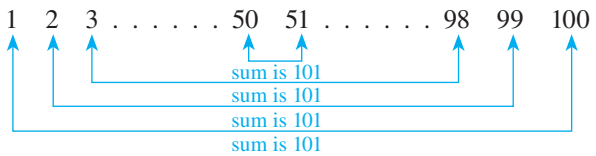
$$\frac{(k+1)(k+2)}{2} = \frac{k^2+3k+2}{2}.$$

Thus the two sides of $P(k+1)$ are equal to the same quantity and so they are equal to each other. Therefore, the equation $P(k+1)$ is true *[as was to be shown].*

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

■

The story is told that one of the greatest mathematicians of all time, Carl Friedrich Gauss (1777–1855), was given the problem of adding the numbers from 1 to 100 by his teacher when he was a young child. The teacher had asked his students to compute the sum, supposedly to gain himself some time to grade papers. But after just a few moments, Gauss produced the correct answer. Needless to say, the teacher was dumbfounded. How could young Gauss have calculated the quantity so rapidly? In his later years, Gauss explained that he had imagined the numbers paired according to the following schema.



The sum of the numbers in each pair is 101, and there are 50 pairs in all; hence the total sum is $50 \cdot 101 = 5{,}050$.

Definition

If a sum with a variable number of terms is shown to equal an expression that does not contain either an ellipsis or a summation symbol, we say that the sum is written **in closed form**.

For example, writing $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$ expresses the sum $1+2+3+\cdots+n$ in closed form.

Example 5.2.2 **Applying the Formula for the Sum of the First *n* Integers**

a. Evaluate $2+4+6+\cdots+500$.

b. Evaluate $5+6+7+8+\cdots+50$.

c. For an integer $h \geq 2$, write $1+2+3+\cdots+(h-1)$ in closed form.

Solution

a. $2+4+6+\cdots+500 = 2\cdot(1+2+3+\cdots+250)$

$$= 2\cdot\left(\frac{250\cdot 251}{2}\right)$$

by applying the formula for the sum of the first n integers with $n = 250$.

$$= 62{,}750$$

b. $5+6+7+8+\cdots+50 = (1+2+3+\cdots+50)-(1+2+3+4)$

$$= \frac{50\cdot 51}{2} - 10 \qquad \text{by applying the formula for the sum of the first } n \text{ integers with } n = 50.$$

$$= 1{,}265$$

c. $1+2+3+\cdots+(h-1) = \dfrac{(h-1)\cdot[(h-1)+1]}{2}$ by applying the formula for the sum of the first n integers with $n = h-1$

$$= \frac{(h-1)\cdot h}{2} \qquad \text{since } (h-1)+1 = h. \quad \blacksquare$$

The next example asks for a proof of another famous and important formula in mathematics—the formula for the sum of a geometric sequence. In a **geometric sequence**, each term is obtained from the preceding one by multiplying by a constant factor. If the first term is 1 and the constant factor is r, then the sequence is $1, r, r^2, r^3, \ldots, r^n, \ldots$. The sum of the first n terms of this sequence is given by the formula

$$\sum_{i=}^{n} r^i = \frac{r^{n+1}-1}{r-1}$$

for every integer $n \geq 0$ and every real number r not equal to 1. The expanded form of the formula is

$$r^0 + r^1 + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1},$$

and because $r^0 = 1$ and $r^1 = r$, the formula for $n \geq 1$ can be rewritten as

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}.$$

Note This is the definition of 0^0 given by Donald E. Knuth in *The Art of Computer Programming, Volume 1: Fundamental Algorithms, 3rd Edition* (Reading, Mass.: Addison-Wesley, 1997), p. 57.

In some mathematical contexts 0^0 is regarded as indeterminate. In discrete mathematics we usually define $0^0 = 1$ so that when we write $\sum_{i=0}^{n} r^i$ we do not need to give special attention to the case $r = 0$.

Example 5.2.3 **Sum of a Geometric Sequence**

Prove that $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$, for every integer $n \geq 0$ and every real number r except 1.

Solution In this example the property $P(n)$ is again an equation, although in this case it contains a real variable r.

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}. \quad \leftarrow \text{the property } (P(n))$$

Because r can be any real number other than 1, the proof begins by supposing that r is a particular but arbitrarily chosen real number not equal to 1. Then the proof continues by mathematical induction on n, starting with $n = 0$. In the basis step, you must show that $P(0)$ is true; that is, you show the property is true for $n = 0$. So you substitute 0 for each n in $P(n)$:

$$\sum_{i=0}^{0} r^i = \frac{r^{0+1}-1}{r-1}. \quad \leftarrow \text{basis } (P(0))$$

In the inductive step, you suppose k is any integer with $k \geq 0$ for which $P(k)$ is true; that is, you suppose the property is true for $n = k$. So you substitute k for each n in $P(n)$:

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}. \quad \leftarrow \text{inductive hypothesis } (P(k))$$

Then you show that $P(k+1)$ is true; that is, you show the property is true for $n = k+1$. So you substitute $k+1$ for each n in $P(n)$:

$$\sum_{i=0}^{k+1} r^i = \frac{r^{(k+1)+1} - 1}{r - 1},$$

or, equivalently,

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}. \quad \leftarrow \text{to show } (P(k+1))$$

In the inductive step for this proof we use another common technique for showing that an equation is true: We start with the left-hand side and transform it step-by-step into the right-hand side. To do so, we use the inductive hypothesis together with algebra and other known facts.

Theorem 5.2.2 Sum of a Geometric Sequence

For any real number r except 1, and any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Proof (by mathematical induction): Suppose r is a particular but arbitrarily chosen real number that is not equal to 1, and let the property $P(n)$ be the equation

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}. \quad \leftarrow P(n)$$

We must show that $P(n)$ is true for every integer $n \geq 0$. We do this by mathematical induction on n.

Show that P(0) is true:

To establish $P(0)$, we must show that

$$\sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1}. \quad \leftarrow P(0)$$

The left-hand side of this equation is $r^0 = 1$ and the right-hand side is

$$\frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1$$

also because $r^1 = r$ and, since $r \neq 1$, $r - 1 \neq 0$. Hence $P(0)$ is true.

Show that for every integer k ≥ 0, if P(k) is true then P(k + 1) is also true:

[Suppose that P(k) is true for a particular but arbitrarily chosen integer $k \geq 0$. That is:]

(continued on page 284)

Note To write $P(0)$, copy $P(n)$ and replace each n by 0.

Let k be any integer with $k \geq 0$, and suppose that

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1} \qquad \leftarrow P(k) \text{ inductive hypothesis}$$

Note To write $P(k)$, copy $P(n)$ and replace each n by k.

[We must show that $P(k+1)$ is true. That is:] We must show that

$$\sum_{i=0}^{k+1} r^i = \frac{r^{(k+1)+1} - 1}{r - 1},$$

or, equivalently, that

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}. \qquad \leftarrow P(k+1)$$

Note To write $P(k+1)$, copy $P(n)$ and replace each n by $k+1$

[We will show that the left-hand side of $P(k+1)$ equals the right-hand side.]

The left-hand side of $P(k+1)$ is

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \sum_{i=0}^{k} r^i + r^{k+1} && \text{by writing the } (k+1)\text{st term separately from the first } k \text{ terms} \\
&= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} && \text{by substitution from the inductive hypothesis} \\
&= \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r-1)}{r-1} && \text{by multiplying the numerator and denominator of the second term by } (r-1) \text{ to obtain a common denominator} \\
&= \frac{(r^{k+1} - 1) + r^{k+1}(r-1)}{r-1} && \text{by adding fractions} \\
&= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r-1} && \text{by multiplying out and using the fact that } r^{k+1} \cdot r = r^{k+1} \cdot r^1 = r^{k+2} \\
&= \frac{r^{k+2} - 1}{r-1} && \text{by canceling the } r^{k+1}\text{'s.}
\end{aligned}$$

which is the right-hand side of $P(k+1)$ *[as was to be shown].*

[Since we have proved the basis step and the inductive step, we conclude that the theorem is true.]

■

Proving an Equality

The proofs of the basis and inductive steps in Examples 5.2.1 and 5.2.3 illustrate two different ways to show that an equation is true: (1) transforming the left-hand side and the right-hand side independently until they are seen to be equal, and (2) transforming one side of the equation until it is seen to be the same as the other side of the equation.

Sometimes people use a method that they believe proves equality but that is actually invalid. For example, to prove the basis step for Theorem 5.2.2, they perform the following steps:

$$\begin{aligned}
\sum_{i=0}^{0} r^i &= \frac{r^{0+1} - 1}{r - 1} \\
r^0 &= \frac{r^1 - 1}{r - 1} \\
1 &= \frac{r-1}{r-1} \\
1 &= 1.
\end{aligned}$$

Caution! Don't try to prove an equality by assuming it is true and deducing a true statement; that form of argument is invalid!

The problem with this method is that starting from a statement and deducing a true conclusion does not prove that the statement is true. A true conclusion can also be deduced from a false statement. For instance, the steps below show how to deduce the true conclusion that $1 = 1$ from the false statement that $1 = 0$:

$$\begin{aligned} 1 &= 0 && \leftarrow \text{false} \\ 0 &= 1 \\ 1+0 &= 0+1 \\ 1 &= 1 && \leftarrow \text{true} \end{aligned}$$

When using mathematical induction to prove formulas, be sure to use a method that avoids invalid reasoning, both for the basis step and for the inductive step.

Deducing Additional Formulas

The formula for the sum of a geometric sequence can be thought of as a family of different formulas in r, one for each real number r except 1.

Example 5.2.4 **Applying the Formula for the Sum of a Geometric Sequence**

In each of (a) and (b) below, assume that m is an integer that is greater than or equal to 3. Write each of the sums in closed form.

a. $1 + 3 + 3^2 + \cdots + 3^{m-2}$

b. $3^2 + 3^3 + 3^4 + \cdots + 3^m$

Solution

a. $$1 + 3 + 3^2 + \cdots + 3^{m-2} = \frac{3^{(m-2)+1} - 1}{3 - 1} = \frac{3^{m-1} - 1}{2}$$ by applying the formula for the sum of a geometric sequence with $r = 3$ and $n = m - 2$

b. $$3^2 + 3^3 + 3^4 + \cdots + 3^m = 3^2 \cdot (1 + 3 + 3^2 + \cdots + 3^{m-2})$$ by factoring out 3^2

$$= 9 \cdot \left(\frac{3^{m-1} - 1}{2} \right)$$ by part (a). ■

As with the formula for the sum of the first n integers, there is a way to think of the formula for the sum of the terms of a geometric sequence that makes it seem simple and intuitive. Let

$$S_n = 1 + r + r^2 + \cdots + r^n.$$

Then

$$rS_n = r + r^2 + r^3 + \cdots + r^{n+1},$$

and so

$$\begin{aligned} rS_n - S_n &= (r + r^2 + r^3 + \cdots + r^{n+1}) - (1 + r + r^2 + \cdots + r^n) \\ &= r^{n+1} - 1. \end{aligned} \tag{5.2.1}$$

Now

$$rS_n - S_n = (r - 1)S_n. \tag{5.2.2}$$

Equating the right-hand sides of equations (5.2.1) and (5.2.2) and dividing by $r-1$ gives

$$S_n = \frac{r^{n+1}-1}{r-1}.$$

This derivation of the formula is quite convincing. However, it is not as logically airtight as the proof by mathematical induction. To go from one step to another in the previous calculations, the argument is made that each term among those indicated by the ellipsis (. . .) has such-and-such an appearance and when these are canceled such-and-such occurs. But it is impossible actually to see each such term and each such calculation, and so the accuracy of these claims cannot be fully checked. With mathematical induction it is possible to focus exactly on what happens in the middle of the ellipsis and verify without doubt that the calculations are correct.

TEST YOURSELF

1. Mathematical induction is a method for proving that a property defined for integers n is true for all values of n that are _____.
2. Let $P(n)$ be a property defined for integers n and consider constructing a proof by mathematical induction for the statement "$P(n)$ is true for all $n \geq a$."
   (a) In the basis step one must show that _____.
   (b) In the inductive step one supposes that _____ for a particular but arbitrarily chosen value of an integer $k \geq a$. This supposition is called the _____. One then has to show that _____.

EXERCISE SET 5.2

1. Use the technique illustrated at the beginning of this section to show that the statements in (a) and (b) are true.
   a. If $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right) = \frac{1}{5}$ then $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{6}\right) = \frac{1}{6}$.
   b. If $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{6}\right) = \frac{1}{6}$ then $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{6}\right)\left(1-\frac{1}{7}\right) = \frac{1}{7}$.

2. For each positive integer n, let $P(n)$ be the formula
   $$1+3+5+\cdots+(2n-1) = n^2.$$
   a. Write $P(1)$. Is $P(1)$ true?
   b. Write $P(k)$.
   c. Write $P(k+1)$.
   d. In a proof by mathematical induction that the formula holds for every integer $n \geq 1$, what must be shown in the inductive step?

3. For each positive integer n, let $P(n)$ be the formula
   $$1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$
   a. Write $P(1)$. Is $P(1)$ true?
   b. Write $P(k)$.
   c. Write $P(k+1)$.
   d. In a proof by mathematical induction that the formula holds for every integer $n \geq 1$, what must be shown in the inductive step?

4. For each integer n with $n \geq 2$, let $P(n)$ be the formula
   $$\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}.$$
   a. Write $P(2)$. Is $P(2)$ true?
   b. Write $P(k)$.
   c. Write $P(k+1)$.
   d. In a proof by mathematical induction that the formula holds for every integer $n \geq 2$, what must be shown in the inductive step?

5. Fill in the missing pieces in the following proof that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

for every integer $n \geq 1$.

Proof: Let the property $P(n)$ be the equation

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2. \quad \leftarrow P(n)$$

Show that P(1) is true: To establish $P(1)$, we must show that when 1 is substituted in place of n, the left-hand side equals the right-hand side. But when $n = 1$, the left-hand side is the sum of all the odd integers from 1 to $2 \cdot 1 - 1$, which is the sum of the odd integers from 1 to 1 and is just 1. The right-hand side is _____(a)_____, which also equals 1. So $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is true: Let k be any integer with $k \geq 1$.

[Suppose P(k) is true. That is:] Suppose

$$1 + 3 + 5 + \cdots + (2k - 1) = \text{\_\_\_(b)\_\_\_}. \quad \leftarrow P(k)$$

[This is the inductive hypothesis.]

[We must show that P(k + 1) is true. That is:] We must show that

$$\text{\_\_\_(c)\_\_\_} = \text{\_\_\_(d)\_\_\_}. \quad \leftarrow P(k+1)$$

Now the left-hand side of $P(k + 1)$ is

$$\begin{aligned} &1 + 3 + 5 + \cdots + (2(k+1) - 1) \\ &\quad = 1 + 3 + 5 + \cdots + (2k + 1) && \text{by algebra} \\ &\quad = [1 + 3 + 5 + \cdots + (2k - 1)] + (2k + 1) \\ &\qquad \text{the next-to-last term is } 2k - 1 \text{ because } \text{\_\_\_(e)\_\_\_} \\ &\quad = k^2 + (2k + 1) && \text{by \_\_\_(f)\_\_\_} \\ &\quad = (k + 1)^2 && \text{by algebra,} \end{aligned}$$

which is the right-hand side of $P(k + 1)$ *[as was to be shown].*

[Since we have proved the basis step and the inductive step, we conclude that the given statement is true.]

Note: This proof was annotated to help make its logical flow more obvious. In standard mathematical writing, such annotation is omitted.

Prove each statement in 6–9 using mathematical induction. Do not derive them from Theorem 5.2.1 or Theorem 5.2.2.

6. For every integer $n \geq 1$,

$$2 + 4 + 6 + \cdots + 2n = n^2 + n.$$

7. For every integer $n \geq 1$,

$$1 + 6 + 11 + 16 + \cdots + (5n - 4) = \frac{n(5n - 3)}{2}.$$

8. For every integer $n \geq 0$,

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

9. For every integer $n \geq 3$,

$$4^3 + 4^4 + 4^5 + \cdots + 4^n = \frac{4(4^n - 16)}{3}.$$

Prove each of the statements in 10–18 by mathematical induction.

10. $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$, for every integer $n \geq 1$.

11. $1^3 + 2^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$, for every integer $n \geq 1$.

12. $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$, for every integer $n \geq 1$.

13. $\displaystyle\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}$, for every integer $n \geq 2$.

14. $\displaystyle\sum_{i=1}^{n+1} i \cdot 2^i = n \cdot 2^{n+2} + 2$, for every integer $n \geq 0$.

H **15.** $\displaystyle\sum_{i=1}^{n} i(i!) = (n+1)! - 1$, for every integer $n \geq 1$.

16. $\left(1 - \dfrac{1}{2^2}\right)\left(1 - \dfrac{1}{3^2}\right) \cdots \left(1 - \dfrac{1}{n^2}\right) = \dfrac{n+1}{2n}$, for every integer $n \geq 2$.

17. $\displaystyle\prod_{i=0}^{n}\left(\frac{1}{2i+1} \cdot \frac{1}{2i+2}\right) = \frac{1}{(2n+2)!}$, for every integer $n \geq 0$.

18. $\displaystyle\prod_{i=2}^{n}\left(1 - \frac{1}{i}\right) = \frac{1}{n}$ for every integer $n \geq 2$.

Hint: See the discussion at the beginning of this section.

19. (For students who have studied calculus) Use mathematical induction, the product rule from calculus, and the facts that $\dfrac{d(x)}{dx} = 1$ and that $x^{k+1} = x \cdot x^k$ to prove that for every integer $n \geq 1$, $\dfrac{d(x^n)}{dx} = nx^{n-1}$.

Use the formula for the sum of the first n integers and/or the formula for the sum of a geometric sequence to evaluate the sums in 20–29 or to write them in closed form.

20. $4 + 8 + 12 + 16 + \cdots + 200$

21. $5 + 10 + 15 + 20 + \cdots + 300$

22. **a.** $3 + 4 + 5 + 6 + \cdots + 1000$
b. $3 + 4 + 5 + 6 + \cdots + m$

23. **a.** $7 + 8 + 9 + 10 + \cdots + 600$
b. $7 + 8 + 9 + 10 + \cdots + k$

24. $1 + 2 + 3 + \cdots + (k - 1)$, where k is any integer with $k \geq 2$.

25. **a.** $1 + 2 + 2^2 + \cdots + 2^{25}$
b. $2 + 2^2 + 2^3 + \cdots + 2^{26}$
c. $2 + 2^2 + 2^3 + \cdots + 2^n$

26. $3 + 3^2 + 3^3 + \cdots + 3^n$, where n is any integer with $n \geq 1$.

27. $5^3 + 5^4 + 5^5 + \cdots + 5^k$, where k is any integer with $k \geq 3$.

28. $1 + \dfrac{1}{2} + \dfrac{1}{2^2} + \cdots + \dfrac{1}{2^n}$, where n is any positive integer.

29. $1 - 2 + 2^2 - 2^3 + \cdots + (-1)^n 2^n$, where n is any positive integer.

30. Observe that

$$\frac{1}{1\cdot 3} = \frac{1}{3}$$
$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} = \frac{2}{5}$$
$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} = \frac{3}{7}$$
$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \frac{1}{7\cdot 9} = \frac{4}{9}.$$

Guess a general formula and prove it by mathematical induction.

31. Compute values of the product

$$\left(1 + \frac{1}{1}\right)\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{3}\right)\cdots\left(1 + \frac{1}{n}\right)$$

for small values of n in order to conjecture a general formula for the product. Prove your conjecture by mathematical induction.

***H* 32.** Observe that

$$1 = 1$$
$$1 - 4 = -(1 + 2)$$
$$1 - 4 + 9 = 1 + 2 + 3$$
$$1 - 4 + 9 - 16 = -(1 + 2 + 3 + 4)$$
$$1 - 4 + 9 - 16 + 25 = 1 + 2 + 3 + 4 + 5.$$

Guess a general formula and prove it by mathematical induction.

***H* 33.** Find a formula in n, a, m, and d for the sum $(a + md) + (a + (m + 1)d) + (a + (m + 2)d) + \cdots + (a + (m + n)d)$, where m and n are integers, $n \geq 0$, and a and d are real numbers. Justify your answer.

34. Find a formula in a, r, m, and n for the sum

$$ar^m + ar^{m+1} + ar^{m+2} + \cdots + ar^{m+n},$$

where m and n are integers, $n \geq 0$, and a and r are real numbers. Justify your answer.

35. You have two parents, four grandparents, eight great-grandparents, and so forth.
a. If all your ancestors were distinct, what would be the total number of your ancestors for the past 40 generations (counting your parents' generation as number one)? (*Hint:* Use the formula for the sum of a geometric sequence.)
b. Assuming that each generation represents 25 years, how long is 40 generations?
c. The total number of people who have ever lived is approximately 10 billion, which equals 10^{10} people. Compare this fact with the answer to part (a). What can you deduce?

Find the mistakes in the proof fragments in 36–38.

36. **Theorem:** For any integer $n \geq 1$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

"**Proof (by mathematical induction):** Certainly the theorem is true for $n = 1$ because $1^2 = 1$ and $\frac{1(1+1)(2\cdot 1+1)}{6} = 1$. So the basis step is true. For the inductive step, suppose that k is any integer with $k \geq 1$, $k^2 = \frac{k(k+1)(2k+1)}{6}$. We must show that $(k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$."

***H* 37.** **Theorem:** For any integer $n \geq 0$,

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

"**Proof (by mathematical induction):**
Let the property $P(n)$ be

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

Show that P(0) is true:
The left-hand side of $P(0)$ is $1 + 2 + 2^2 + \cdots + 2^0 = 1$ and the right-hand side is $2^{0+1} - 1 = 2 - 1 = 1$ also. So $P(0)$ is true."

H 38. **Theorem:** For any integer $n \geq 1$,

$$\sum_{i=1}^{n} i(i!) = (n+1)! - 1.$$

"**Proof (by mathematical induction): Let the property**

$$P(n) \text{ be } \sum_{i=1}^{n} i(i!) = (n+1)! - 1.$$

Show that P*(1) *is true: When $n = 1$,

$$\sum_{i=1}^{i} i(i!) = (1+1)! - 1.$$

So $1(1!) = 2! - 1$
and $1 = 1.$
Thus $P(1)$ is true."

***39.** Use Theorem 5.2.1 to prove that if m and n are any positive integers and m is odd, then $\sum_{k=0}^{m-1} (n+k)$ is divisible by m. Does the conclusion hold if m is even? Justify your answer.

H* 40. Use Theorem 5.2.1 and the result of exercise 10 to prove that if p is any prime number with $p \geq 5$, then the sum of the squares of any p consecutive integers is divisible by p.

ANSWERS FOR TEST YOURSELF

1. greater than or equal to some initial value **2.** (a) $P(a)$ is true (b) $P(k)$ is true; inductive hypothesis; $P(k+1)$ is true

5.3 Mathematical Induction II: Applications

[Mathematical induction is] the standard proof technique in computer science.
—Anthony Ralston, 1984

In Section 5.2 we showed how to use mathematical induction to prove formulas. In this section we will show how to apply it in a broader variety of situations.

As a first example consider the argument that the U.S. penny should be eliminated because it isn't profitable to produce. Due to inflation and the rising cost of metals, it actually costs more than one cent to produce a penny. If the penny were eliminated and another coin worth 3¢ were introduced, what prices could be paid using only 3¢ and 5¢ coins? The table below shows some examples.

Number of Cents	How to Obtain It
3¢	3¢
5¢	5¢
8¢	3¢ + 5¢
9¢	3¢ + 3¢ + 3¢
10¢	5¢ + 5¢
11¢	3¢ + 3¢ + 5¢
12¢	3¢ + 3¢ + 3¢ + 3¢
13¢	3¢ + 5¢ + 5¢
14¢	3¢ + 3¢ + 3¢ + 5¢
15¢	5¢ + 5¢ + 5¢
16¢	3¢ + 3¢ + 5¢ + 5¢
17¢	3¢ + 3¢ + 3¢ + 3¢ + 5¢

Can the table be continued indefinitely to show that every larger price could be paid with the two coins? This question is similar to the one raised in the opening example in Section 5.2, which involved showing that if the property illustrated in the table was true for an arbitrarily chosen row k, then it was also true for row $k + 1$. To use a similar technique for this example, suppose that a collection of coins worth $k¢$ can be obtained using $3¢$ and $5¢$ coins. The challenge is to show that a collection of coins worth $(k + 1)¢$ can be obtained using $3¢$ and $5¢$ coins.

To meet the challenge observe that just one of two situations must occur: either the collection worth $k¢$ contains a $5¢$ coin or it does not. If you can obtain $k¢$ using at least one $5¢$ coin, then you can obtain $(k + 1)¢$ by replacing the $5¢$ coin by two $3¢$ coins, as shown in Figure 5.3.1.

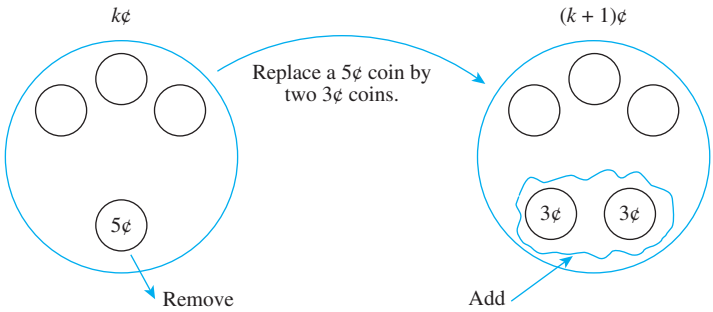


FIGURE 5.3.1

On the other hand, if you can obtain $k¢$ without using a $5¢$ coin, then you need to use $3¢$ coins exclusively. If the total is more than $8¢$, then three or more $3¢$ coins must be included, in which case you can replace three of the $3¢$ coins by two $5¢$ coins to obtain a total of $(k + 1)¢$, as shown in Figure 5.3.2.

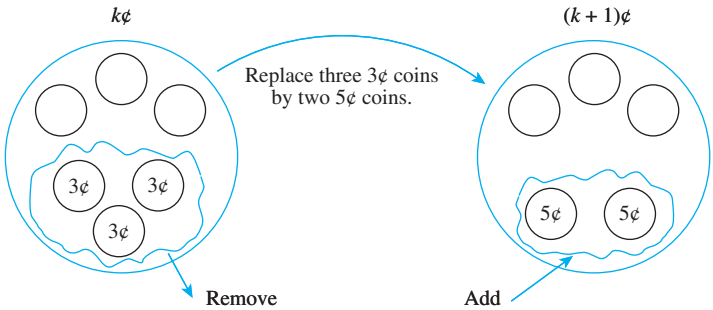


FIGURE 5.3.2

This discussion shows that for any integer k that is at least 8, if you can obtain $k¢$ using $3¢$ and $5¢$ coins, then you can obtain $(k + 1)¢$ using $3¢$ and $5¢$ coins. This is essentially the inductive step of a proof by mathematical induction, and the fact that you can obtain $8¢$ using one $3¢$ and one $5¢$ coin provides the basis step for the induction.

In Section 5.2 the properties proved by mathematical induction were all equations. In this section the properties are more general sentences. For this example the sentence is "$n¢$ can be obtained using $3¢$ and $5¢$ coins," and the proof by mathematical induction shows that the sentence is true for every integer greater than or equal to 8.

Proposition 5.3.1

For every integer $n \geq 8$, $n¢$ can be obtained using $3¢$ and $5¢$ coins.

Proof (by mathematical induction):

Let the property $P(n)$ be the sentence

$n¢$ can be obtained using $3¢$ and $5¢$ coins. ← $P(n)$

Show that P(8) is true:

Note To write $P(8)$, just copy $P(n)$ and replace each n by 8.

$P(8)$ is true because $8¢$ can be obtained using one $3¢$ coin and one $5¢$ coin.

Show that for every integer $k \geq 8$, if $P(k)$ is true then $P(k+1)$ is also true:

[Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 8$. That is:] Suppose that k is any integer with $k \geq 8$ such that

Note To write $P(k)$, just copy $P(n)$ and replace each n by k.

$k¢$ can be obtained using $3¢$ and $5¢$ coins. ← $P(k)$ inductive hypothesis

[We must show that $P(k+1)$ is true. That is:] We must show that

Note To write $P(k+1)$, just copy $P(n)$ and replace each n by $k+1$.

$(k+1)¢$ can be obtained using $3¢$ and $5¢$ coins. ← $P(k+1)$

Case 1 (There is a $5¢$ coin among those used to make up the $k¢$.): In this case replace the $5¢$ coin by two $3¢$ coins; the result will be $(k+1)¢$.

Case 2 (There is not a $5¢$ coin among those used to make up the $k¢$.): In this case, because $k \geq 8$, at least three $3¢$ coins must have been used. So remove three $3¢$ coins and replace them by two $5¢$ coins; the result will be $(k+1)¢$.

Thus in either case $(k+1)¢$ can be obtained using $3¢$ and $5¢$ coins *[as was to be shown].*

[Since we have proved the basis step and the inductive step, we conclude that the proposition is true.]

The basic outlines of the proofs in the remainder of this section are the same in all cases, but the details of the basis and inductive steps differ quite a lot from one to another.

Example 5.3.1 **Proving a Divisibility Property**

Use mathematical induction to prove that for each integer $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Solution As in the previous proofs by mathematical induction, you need to identify the property $P(n)$. In this example, $P(n)$ is the sentence

$2^{2n} - 1$ is divisible by 3. ← the property ($P(n)$)

By substitution, the statement for the basis step, $P(0)$, is

$2^{2 \cdot 0} - 1$ is divisible by 3. ← basis ($P(0)$)

The supposition for the inductive step, $P(k)$, is

$2^{2k} - 1$ is divisible by 3, ← inductive hypothesis ($P(k)$)

and the conclusion to be shown, $P(k+1)$, is

$2^{2(k+1)} - 1$ is divisible by 3. ← to show ($P(k+1)$)

Recall that an integer m is divisible by 3 if, and only if, $m = 3r$ for some integer r. Now the statement $P(0)$ is true because $2^{2\cdot 0} - 1 = 2^0 - 1 = 1 - 1 = 0$, which is divisible by 3 because $0 = 3 \cdot 0$.

To prove the inductive step, you suppose that k is any integer greater than or equal to 0 such that $P(k)$ is true. In other words, you suppose that $2^{2k} - 1$ is divisible by 3. You must then prove the truth of $P(k+1)$. Thus, you must show that $2^{2(k+1)} - 1$ is divisible by 3. Now

$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\ &= 2^{2k} \cdot 2^2 - 1 \quad \text{by the laws of exponents.} \\ &= 2^{2k} \cdot 4 - 1. \end{aligned}$$

Your aim is to show that $2^{2k} \cdot 4 - 1$ is divisible by 3, but why should that be so? Both $2^{2k} \cdot 4 - 1$ and $2^{2k} - 1$ have a lot in common, and, by the inductive hypothesis, $2^{2k} - 1$ is divisible by 3. Observe what happens if you subtract $2^{2k} - 1$ from $2^{2k} \cdot 4 - 1$:

$$\underbrace{2^{2k} \cdot 4 - 1}_{\text{divisible by 3?}} - \underbrace{(2^{2k} - 1)}_{\text{divisible by 3}} = \underbrace{2^{2k} \cdot 3}_{\text{divisible by 3}}.$$

Adding $2^{2k} - 1$ to both sides gives

$$\underbrace{2^{2k} \cdot 4 - 1}_{\text{divisible by 3?}} = \underbrace{2^{2k} \cdot 3}_{\text{divisible by 3}} + \underbrace{(2^{2k} - 1)}_{\text{divisible by 3}}.$$

Both terms of the sum on the right-hand side of this equation are divisible by 3; hence the sum is divisible by 3. (See exercise 15 of Section 4.3.) Therefore, the left-hand side of the equation is also divisible by 3, which is what was to be shown.

This discussion is summarized as follows:

Proposition 5.3.2

For each integer $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proof (by mathematical induction): Let the property $P(n)$ be the sentence "$2^{2n} - 1$ is divisible by 3."

$$2^{2n} - 1 \text{ is divisible by 3.} \qquad \leftarrow P(n)$$

Show that P(0) is true:
To establish $P(0)$, we must show that

Note To write $P(0)$, just copy $P(n)$ and replace each n by 0.

$$2^{2\cdot 0} - 1 \text{ is divisible by 3.} \qquad \leftarrow P(0)$$

But

$$2^{2\cdot 0} - 1 = 2^0 - 1 = 1 - 1 = 0,$$

and 0 is divisible by 3 because $0 = 3 \cdot 0$. Hence $P(0)$ is true.

Show that for any integer k ≥ 0, if P(k) is true then P(k + 1) is also true:
[Suppose that P(k) is true for a particular but arbitrarily chosen integer $k \geq 0$. That is:]
Let k be any integer with $k \geq 0$, and suppose that

Note To write $P(k)$, just copy $P(n)$ and replace each n by k.

$$2^{2k} - 1 \text{ is divisible by 3.} \qquad \leftarrow P(k) \text{ inductive hypothesis}$$

By definition of divisibility, this means that

$$2^{2k} - 1 = 3r \quad \text{for some integer } r.$$

[We must show that $P(k+1)$ is true. That is:] We must show that

$$2^{2(k+1)} - 1 \text{ is divisible by 3.} \quad \leftarrow P(k+1)$$

Note To write $P(k+1)$, just copy $P(n)$ and replace each n by $k+1$.

Now

$$\begin{aligned}
2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\
&= 2^{2k} \cdot 2^2 - 1 && \text{by the laws of exponents} \\
&= 2^{2k} \cdot 4 - 1 \\
&= 2^{2k}(3+1) - 1 \\
&= 2^{2k} \cdot 3 + (2^{2k} - 1) && \text{by the laws of algebra} \\
&= 2^{2k} \cdot 3 + 3r && \text{by inductive hypothesis} \\
&= 3(2^{2k} + r) && \text{by factoring out the 3.}
\end{aligned}$$

But $2^{2k} + r$ is an integer because it is a sum of products of integers, and so, by definition of divisibility, $2^{2(k+1)} - 1$ is divisible by 3 *[as was to be shown].*
[Since we have proved the basis step and the inductive step, we conclude that the proposition is true.]

■

Another way to prove the inductive step for a divisibility property is illustrated in the answer for exercise 11 at the end of this section. It is shown in Appendix B.

Example 5.3.2 **Proving an Inequality**

Use mathematical induction to prove that for each integer $n \geq 3$,

$$2^n + 1 < 2^n.$$

Solution In this example the property $P(n)$ is the inequality

$$\boxed{2n + 1 < 2^n.} \quad \leftarrow \text{the property } (P(n))$$

By substitution, the statement for the basis step, $P(3)$, is

$$\boxed{2 \cdot 3 + 1 < 2^3.} \quad \leftarrow \text{basis } (P(3))$$

The supposition for the inductive step, $P(k)$, is

$$\boxed{2k + 1 < 2^k,} \quad \leftarrow \text{inductive hypothesis } (P(k))$$

and the conclusion to be shown is

$$\boxed{2(k+1) + 1 < 2^{k+1}.} \quad \leftarrow \text{to show } (P(k+1))$$

To prove the basis step, observe that the statement $P(3)$ is true because $2 \cdot 3 + 1 = 7$, $2^3 = 8$, and $7 < 8$.

For the inductive step you assume the inductive hypothesis that for a particular but arbitrarily chosen integer $k \geq 3$, $2k + 1 < 2^k$, and then you must show that $2k + 1 < 2^{k+1}$. With inequality proofs you can often apply the inductive hypothesis at an early stage. In this case, you can substitute from the induction hypothesis to obtain

$$2(k+1) + 1 \;=\; (2k+1) + 2 < 2^k + 2.$$

At this point you need to think about your goal. You want the right-hand side of the inequality to be 2^{k+1}. Since you already know that $2(k+1)+1 < 2^k + 2$, an easy way to complete your job would be to show that

$$2^k + 2 < 2^{k+1}.$$

But this inequality is true because $2 < 2^k$ for $k \geq 3$, and thus

$$2^k + 2 < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

by algebra and a law of exponents. Transitivity of order then implies that $2(k+1)+1 < 2^{k+1}$. This discussion is summarized in the following formal proof.

Note Properties of order are listed in Appendix A.

Proposition 5.3.3

For every integer $n \geq 3$, $2n + 1 < 2^n$.

Proof (by mathematical induction):

Let the property $P(n)$ be the inequality

$$2n + 1 < 2^n. \qquad \leftarrow P(n)$$

Show that P(3) is true:

To establish $P(3)$, we must show that

$$2 \cdot 3 + 1 < 2^3. \qquad \leftarrow P(3)$$

Note For $P(3)$, copy $P(n)$ and replace each n by 3.

Now

$$2 \cdot 3 + 1 = 7 \quad \text{and} \quad 2^3 = 8 \quad \text{and} \quad 7 < 8.$$

Hence $P(3)$ is true.

Show that for every integer k ≥ 3, if P(k) is true then P(k + 1) is also true:

[Suppose that P(k) is true for a particular but arbitrarily chosen integer $k \geq 3$. That is:]

Suppose that k is any integer with $k \geq 3$ such that

$$2k + 1 < 2^k. \qquad \leftarrow P(k) \text{ inductive hypothesis}$$

Note For $P(k)$, copy $P(n)$ and replace each n by k.

[We must show that $P(k+1)$ is true. That is:] We must show that

$$2(k+1) + 1 < 2^{(k+1)}. \qquad \leftarrow P(k+1)$$

Note For $P(k+1)$, copy $P(n)$ and replace each n by $k+1$.

Now

$$\begin{aligned}
2(k+1) + 1 &= 2k + 1 + 2 && \text{by algebra} \\
&< 2^k + 2 && \text{because, by the inductive hypothesis, } 2k+1 < 2^k \\
&< 2^k + 2^k && \text{because } 2 < 2^k \text{ since } k \geq 3 \\
&= 2 \cdot 2^k && \text{by algebra} \\
&= 2^{k+1} && \text{by the laws of exponents.}
\end{aligned}$$

Thus by transitivity of order $2(k+1)+1 < 2^{k+1}$ *[as was to be shown].*

[Since we have proved the basis step and the inductive step, we conclude that the proposition is true.]

■

The next example demonstrates how to use mathematical induction to show that the terms of a sequence satisfy a certain explicit formula.

Example 5.3.3 **Proving a Property of a Sequence**

Define a sequence $a_1, a_2, a_3, \ldots$ as follows:*

$$a_1 = 2$$
$$a_k = 5a_{k-1} \quad \text{for every integer } k \geq 2.$$

a. Write the first four terms of the sequence.

b. It is claimed that for each integer $n \geq 0$, the nth term of the sequence has the same value as that given by the formula $2 \cdot 5^{n-1}$. In other words, the claim is that the terms of the sequence satisfy the equation $a_n = 2 \cdot 5^{n-1}$. Prove that this is true.

Solution

a. $a_1 = 2$
$a_2 = 5a_{2-1} = 5a_1 = 5 \cdot 2 = 10$
$a_3 = 5a_{3-1} = 5a_2 = 5 \cdot 10 = 50$
$a_4 = 5a_{4-1} = 5a_3 = 5 \cdot 50 = 250$

b. To use mathematical induction to show that every term of the sequence satisfies the equation, begin by showing that the first term of the sequence satisfies the equation. Then suppose that an arbitrarily chosen term a_k satisfies the equation and prove that the next term a_{k+1} also satisfies the equation.

Proof (by mathematical induction):

Let $a_1, a_2, a_3, \ldots$ be the sequence defined by specifying that $a_1 = 2$ and $a_k = 5a_{k-1}$ for every integer $k \geq 2$, and let the property $P(n)$ be the equation

$$a_n = 2 \cdot 5^{n-1}. \qquad \leftarrow P(n)$$

We will use mathematical induction to prove that for every integer $n \geq 1$, $P(n)$ is true.

Show that P(1) is true:

To establish $P(1)$, we must show that

Note For $P(1)$, copy $P(n)$ and replace each n by 1.

$$a_1 = 2 \cdot 5^{1-1}. \qquad \leftarrow P(1)$$

Now the left-hand side of $P(1)$ is

$$a_1 = 2 \qquad \text{by definition of } a_1, a_2, a_3, \ldots,$$

and the right-hand side of $P(1)$ is

$$2 \cdot 5^{1-1} = 2 \cdot 5^0 = 2 \cdot 1 = 2.$$

Thus the two sides of $P(1)$ are equal to the same quantity, and hence $P(1)$ is true.

Show that for each integer k ≥ 1, if P(k) is true then P(k + 1) is also true:

[Suppose that P(k) is true for a particular but arbitrarily chosen integer k ≥ 1. That is:] Let k be any integer with $k \geq 1$, and suppose that

Note For $P(k)$, copy $P(n)$ and replace each n by k.

$$a_k = 2 \cdot 5^{k-1}. \qquad \leftarrow P(k)$$
inductive hypothesis

[We must show that $P(k+1)$ is true. That is:] We must show that

$$a_{k+1} = 2 \cdot 5^{(k+1)-1},$$

*This is another example of a recursive definition. The general subject of recursion is discussed in Section 5.6.

or, equivalently,

$$a_{k+1} = 2 \cdot 5^k. \qquad \leftarrow P(k+1)$$

Note For $P(k+1)$, copy $P(n)$ and replace each n by $k+1$.

But the left-hand side of $P(k+1)$ is

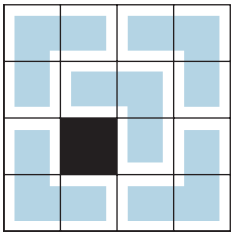
$$\begin{aligned} a_{k+1} &= 5a_{(k+1)-1} && \text{by definition of } a_1, a_2, a_3, \ldots \\ &= 5a_k && \text{since } (k+1)-1 = k \\ &= 5 \cdot (2 \cdot 5^{k-1}) && \text{by inductive hypothesis} \\ &= 2 \cdot (5 \cdot 5^{k-1}) && \text{by regrouping} \\ &= 2 \cdot 5^k && \text{by the laws of exponents,} \end{aligned}$$

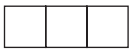
which is the right-hand side of $P(k+1)$ *[as was to be shown].*

[Since we have proved the basis step and the inductive step, we conclude that the formula holds for all terms of the sequence.] ■

A Problem with Trominoes

The word *polyomino*, a generalization of *domino*, was introduced by Solomon Golomb in 1954 when he was a 22-year-old university student. Subsequently, he and others proved many interesting properties about them, and they became the basis for the popular computer game Tetris. A particular type of polyomino, called a *tromino*, is made up of three attached squares, which can be of two types:



straight  and L-shaped 

Call a checkerboard that is formed using m squares on a side an $m \times m$ ("m by m") checkerboard. Observe that if one square is removed from a 4×4 checkerboard, the remaining squares can be completely covered by L-shaped trominoes. For instance, a covering for one such board is illustrated in the figure to the left.

In his first article about polyominoes, Golomb included a proof of the following theorem. It is a beautiful example of an argument by mathematical induction.

Theorem 5.3.4 Covering a Board with Trominoes

For any integer $n \geq 1$, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be completely covered by L-shaped trominoes.

The main insight leading to a proof of this theorem is the observation that because $2^{k+1} = 2 \cdot 2^k$, when a $2^{k+1} \times 2^{k+1}$ board is split in half both vertically and horizontally, each half side will have length 2^k and so each resulting quadrant will be a $2^k \times 2^k$ checkerboard.

Proof (by mathematical induction):

Let the property $P(n)$ be the sentence

> If any square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be completely covered by L-shaped trominoes. $\leftarrow P(n)$

Note Even when $P(n)$ is a long sentence, $P(1)$, $P(k)$, and $P(k+1)$ are each obtained by copying $P(n)$ and replacing each n by 1, k, $k+1$, respectively.

Show that P(1) is true:
A $2^1 \times \times 2^1$ checkerboard just consists of four squares. If one square is removed, the remaining squares form an L, which can be covered by a single L-shaped tromino, as illustrated in the figure to the left. Hence $P(1)$ is true.

Show that for every integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is also true:

[Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 3$. That is:] Let k be any integer such that $k \geq 1$, and suppose that

> If any square is removed from a $2^k \times 2^k$ checkerboard, then the remaining squares can be completely covered by L-shaped trominoes. ← $P(k)$

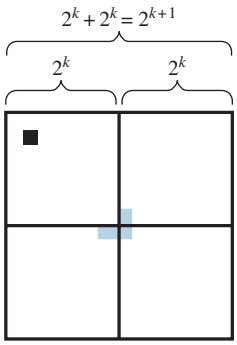
$P(k)$ is the inductive hypothesis.

[We must show that $P(k+1)$ is true. That is:] We must show that

> If any square is removed from a $2^{k+1} \times 2^{k+1}$ checkerboard, then the remaining squares can be completely covered by L-shaped trominoes. ← $P(k+1)$

Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Divide it into four equal quadrants: Each will consist of a $2^k \times 2^k$ checkerboard. In one of the quadrants, one square will have been removed, and so, by inductive hypothesis, all the remaining squares in this quadrant can be completely covered by L-shaped trominoes.

The other three quadrants meet at the center of the checkerboard, and the center of the checkerboard serves as a corner of a square from each of those quadrants. An L-shaped tromino can, therefore, be placed on those three central squares. This situation is illustrated in the figure to the left.



By inductive hypothesis, the remaining squares in each of the three quadrants can be completely covered by L-shaped trominoes. Thus every square in the $2^{k+1} \times 2^{k+1}$ checkerboard except the one that was removed can be completely covered by L-shaped trominoes *[as was to be shown].*

TEST YOURSELF

1. Mathematical induction differs from the kind of induction used in the natural sciences because it is actually a form of _____ reasoning.
2. Mathematical induction can be used to _____ conjectures that have been made using inductive reasoning.

EXERCISE SET 5.3

1. Use mathematical induction (and the proof of proposition 5.3.1 as a model) to show that any amount of money of at least 14¢ can be made up using 3¢ and 8¢ coins.
2. Use mathematical induction to show that any postage of at least 12¢ can be obtained using 3¢ and 7¢ stamps.
3. Stamps are sold in packages containing either 5 stamps or 8 stamps.
   a. Show that a person can obtain 5, 8, 10, 13, 15, 16, 20, 21, 24, or 25 stamps by buying a collection of 5-stamp packages and 8-stamp packages.
   b. Use mathematical induction to show that any quantity of at least 28 stamps can be obtained

by buying a collection of 5-stamp packages and 8-stamp packages.

4. For each positive integer n, let $P(n)$ be the sentence that describes the following divisibility property:

$$5^n - 1 \text{ is divisible by 4.}$$

a. Write $P(0)$. Is $P(0)$ true?
b. Write $P(k)$.
c. Write $P(k+1)$.
d. In a proof by mathematical induction that this divisibility property holds for every integer $n \geq 0$, what must be shown in the inductive step?

5. For each positive integer n, let $P(n)$ be the inequality

$$2^n < (n+1)!.$$

a. Write $P(2)$. Is $P(2)$ true?
b. Write $P(k)$.
c. Write $P(k+1)$.
d. In a proof by mathematical induction that this inequality holds for every integer $n \geq 2$, what must be shown in the inductive step?

6. For each positive integer n, let $P(n)$ be the sentence

Any checkerboard with dimensions $2 \times 3n$ can be completely covered with L-shaped trominoes.

a. Write $P(1)$. Is $P(1)$ true?
b. Write $P(k)$.
c. Write $P(k+1)$.
d. In a proof by mathematical induction that $P(n)$ is true for each integer $n \geq 1$, what must be shown in the inductive step?

7. For each positive integer n, let $P(n)$ be the sentence

In any round-robin tournament involving n teams, the teams can be labeled $T_1, T_2, T_3, \ldots, T_n$, so that T_i beats T_{i+1} for every $i = 1, 2, \ldots, n$.

a. Write $P(2)$. Is $P(2)$ true?
b. Write $P(k)$.
c. Write $P(k+1)$.
d. In a proof by mathematical induction that $P(n)$ is true for each integer $n \geq 2$, what must be shown in the inductive step?

Prove each statement in 8–23 by mathematical induction.

8. $5^n - 1$ is divisible by 4, for every integer $n \geq 0$.

9. $7^n - 1$ is divisible by 6, for each integer $n \geq 0$.

10. $n^3 - 7n + 3$ is divisible by 3, for each integer $n \geq 0$.

11. $3^{2n} - 1$ is divisible by 8, for each integer $n \geq 0$.

12. For any integer $n \geq 0$, $7^n - 2^n$ is divisible by 5.

H 13. For any integer $n \geq 0$, $x^n - y^n$ is divisible by $x - y$, where x and y are any integers with $x \neq y$.

H 14. $n^3 - n$ is divisible by 6, for each integer $n \geq 0$.

15. $n(n^2 + 5)$ is divisible by 6, for each integer $n \geq 0$.

16. $2^n < (n+1)!$, for every integer $n \geq 2$.

17. $1 + 3n \leq 4^n$, for every integer $n \geq 0$.

18. $5^n + 9 < 6^n$, for each integer $n \geq 2$.

19. $n^2 < 2^n$, for every integer $n \geq 5$.

20. $2^n < (n+2)!$, for each integer $n \geq 0$.

21. $\sqrt{n} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}}$, for every integer $n \geq 2$.

22. $1 + nx \leq (1+x)^n$, for every real number $x > -1$ and every integer $n \geq 2$.

23. **a.** $n^3 > 2n + 1$, for each integer $n \geq 2$.
b. $n! > n^2$, for each integer $n \geq 4$.

24. A sequence $a_1, a_2, a_3, \ldots$ is defined by letting $a_1 = 3$ and $a_k = 7a_{k-1}$ for each integer $k \geq 2$. Show that $a_n = 3 \cdot 7^{n-1}$ for every integer $n \geq 1$.

25. A sequence $b_0, b_1, b_2, \ldots$ is defined by letting $b_0 = 5$ and $b_k = 4 + b_{k-1}$ for each integer $k \geq 1$. Show that $b_n > 4n$ for every integer $n \geq 0$.

26. A sequence $c_0, c_1, c_2, \ldots$ is defined by letting $c_0 = 3$ and $c_k = (c_{k-1})^2$ for every integer $k \geq 1$. Show that $c_n = 3^{2n}$ for each integer $n \geq 0$.

27. A sequence $d_1, d_2, d_3, \ldots$ is defined by letting $d_1 = 2$ and $d_k = \frac{d_{k-1}}{k}$ for each integer $k \geq 2$. Show that for every integer $n \geq 1$, $d_n = \frac{2}{n!}$.

28. Prove that for every integer $n \geq 1$,

$$\frac{1}{3} = \frac{1 + 3 + 5 + \cdots + (2n-1)}{(2n+1)(2n+3) + \cdots + (2n + (2n-1))}.$$

Exercises 29 and 30 use the definition of string and string length from page 13 in Section 1.4. Recursive definitions for these terms are given in Section 5.9.

29. A set L consists of strings obtained by juxtaposing one or more of *abb*, *bab*, and *bba*. Use mathematical induction to prove that for every integer $n \geq 1$, if a string s in L has length $3n$, then s contains an even number of *b*'s.

30. A set S consists of strings obtained by juxtaposing one or more copies of 1110 and 0111. Use mathematical induction to prove that for every integer $n \geq 1$, if a string s in S has length $4n$, then the number of 1's in s is a multiple of 3.

31. Use mathematical induction to give an alternative proof for the statement proved in Example 4.9.9: For any positive integer n, a complete graph on n vertices has $\frac{n(n-1)}{2}$ edges. *Hint:* Let $P(n)$ be the sentence, "the number of edges in a complete graph on n vertices is $\frac{n(n-1)}{2}$."

H 32. Some 5×5 checkerboards with one square removed can be completely covered by L-shaped trominoes, whereas other 5×5 checkerboards cannot. Find examples of both kinds of checkerboards. Justify your answers.

33. Consider a 4×6 checkerboard. Draw a covering of the board by L-shaped trominoes.

H 34. a. Use mathematical induction to prove that for each integer $n \geq 1$, any checkerboard with dimensions $2 \times 3n$ can be completely covered with L-shaped trominoes.

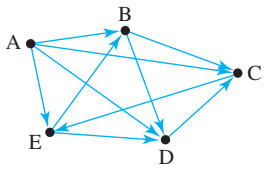
b. Let n be any integer greater than or equal to 1. Use the result of part (a) to prove by mathematical induction that for every integer m, any checkerboard with dimensions $2m \times 3n$ can be completely covered with L-shaped trominoes.

35. Let m and n be any integers that are greater than or equal to 1.

a. Prove that a necessary condition for an $m \times n$ checkerboard to be completely coverable by L-shaped trominoes is that mn be divisible by 3.

H b. Prove that having mn be divisible by 3 is not a sufficient condition for an $m \times n$ checkerboard to be completely coverable by L-shaped trominoes.

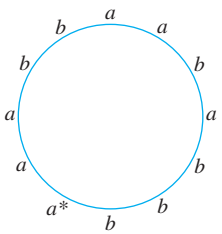
36. In a round-robin tournament each team plays every other team exactly once with ties not allowed. If the teams are labeled $T_1, T_2, \ldots, T_n$, then the outcome of such a tournament can be represented by a directed graph, in which the teams are represented as dots and an arrow is drawn from one dot to another if, and only if, the following team represented by the first dot beats the team represented by the second dot. For example, the following directed graph shows one outcome of a round-robin tournament involving five teams, A, B, C, D, and E.



Use mathematical induction to show that in any round-robin tournament involving n teams, where $n \geq 2$, it is possible to label the teams $T_1, T_2, \ldots, T_n$ so that T_i beats T_{i+1} for all $i = 1, 2, \ldots, n-1$. (For instance, one such labeling in the example above is $T_1 = A$, $T_2 = B$, $T_3 = C$, $T_4 = E$, $T_5 = D$.) (*Hint:* Given $k+1$ teams, pick one—say T'—and apply the inductive hypothesis to the remaining teams to obtain an ordering $T_1, T_2, \ldots, T_k$. Consider three cases: T' beats T_1, T' loses to the first m teams (where $1 \leq m \leq k-1$) and beats the $(m+1)$st team, and T' loses to all the other teams.)

H* 37. On the outside rim of a circular disk the integers from 1 through 30 are painted in random order. Show that no matter what this order is, there must be three successive integers whose sum is at least 45.

H 38. Suppose that n a's and n b's are distributed around the outside of a circle. Use mathematical induction to prove that for any integer $n \geq 1$, given any such arrangement, it is possible to find a starting point so that if you travel around the circle in a clockwise direction, the number of a's you pass is never less than the number of b's you have passed. For example, in the diagram shown below, you could start at the a with an asterisk.



39. For a polygon to be **convex** means that given any two points on or inside the polygon, the line joining the points lies entirely inside the polygon. Use mathematical induction to prove that for every integer $n \geq 3$, the angles of any n-sided convex polygon add up to $180(n-2)$ degrees.

40. a. Prove that in an 8×8 checkerboard with alternating black and white squares, if the squares in the top right and bottom left corners are

removed the remaining board cannot be covered with dominoes. (*Hint:* Mathematical induction is not needed for this proof.)

H **b.** Use mathematical induction to prove that for each positive integer n, if a $2n \times 2n$ checkerboard with alternating black and white squares has one white square and one black square removed anywhere on the board, the remaining squares can be covered with dominoes.

H **41.** A group of people are positioned so that the distance between any two people is different from the distance between any other two people. Suppose that the group contains an odd number of people and each person sends a message to their nearest neighbor. Use mathematical induction to prove that at least one person does not receive a message from anyone. [This exercise is inspired by the article "Odd Pie Fights" by L. Carmony, *The Mathematics Teacher*, **72**(1), 1979, 61–64.]

42. Show that for any even integer n, it is possible to find a group of n people who are all positioned so that the distance between any two people is different from the distance between any other two people, so that each person sends a message to their nearest neighbor, and so that every person in the group receives a message from another person in the group.

43. Define a game as follows: You begin with an urn that contains a mixture of white and black balls, and during the game you have access to as many additional white and black balls as you might need. In each move you remove two balls from the urn without looking at their colors. If the balls are the same color, you put in one black ball. If the balls are different colors, you put the white ball back into the urn and keep the black ball out. Because each move reduces the number of balls in the urn by one, the game will end with a single ball in the urn. If you know how many white balls and how many black balls are initially in the urn, can you predict the color of the ball at the end of the game? [This exercise is based on one described in "Why correctness must be a mathematical concern" by E. W. Dijkstra, www.cs.utexas.edu/users/EWD/transcriptions/EWD07xx/EWD720.html.]

H **a.** Map out all possibilities for playing the game starting with two balls in the urn, then three balls, and then four balls. For each case keep track of the number of white and black balls you start with and the color of the ball at the end of the game.

H **b.** Does the number of white balls seem to be predictive? Does the number of black balls seem to be predictive? Make a conjecture about the color of the ball at the end of the game given the numbers of white and black balls at the beginning.

c. Use mathematical induction to prove the conjecture you made in part (b).

44. Let $P(n)$ be the following sentence: Given any graph G with n vertices satisfying the condition that every vertex of G has degree at most M, then the vertices of G can be colored with at most $M + 1$ colors in such a way that no two adjacent vertices have the same color. Use mathematical induction to prove this statement is true for every integer $n \geq 1$.

In order for a proof by mathematical induction to be valid, the basis statement must be true for $n = a$ and the argument of the inductive step must be correct for every integer $k \geq a$. In 45 and 46 find the mistakes in the "proofs" by mathematical induction.

45. "**Theorem:**" For any integer $n \geq 1$, all the numbers in a set of n numbers are equal to each other.

"**Proof (by mathematical induction):** It is obviously true that all the numbers in a set consisting of just one number are equal to each other, so the basis step is true. For the inductive step, let $A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$ be any set of $k + 1$ numbers. Form two subsets each of size k:

$$B = \{a_1, a_2, a_3, \ldots, a_k\} \text{ and}$$
$$C = \{a_1, a_3, a_4, \ldots, a_{k+1}\}.$$

(B consists of all the numbers in A except a_{k+1}, and C consists of all the numbers in A except a_2.) By inductive hypothesis, all the numbers in B equal a_1 and all the numbers in C equal a_1 (since both sets have only k numbers). But every number in A is in B or C, so all the numbers in A equal a_1; hence all are equal to each other."

H **46.** "**Theorem:**" For every integer $n \geq 1$, $3^n - 2$ is even.
"**Proof (by mathematical induction):** Suppose the theorem is true for an integer k, where $k \geq 1$. That is, suppose that $3^k - 2$ is even. We must show that $3^{k+1} - 2$ is even. Observe that

$$3^{k+1} - 2 = 3^k \cdot 3 - 2 = 3^k(1 + 2) - 2$$
$$= (3^k - 2) + 3^k \cdot 2.$$

Now $3^k - 2$ is even by inductive hypothesis and $3^k \cdot 2$ is even by inspection. Hence the sum of the two quantities is even (by Theorem 4.1.1). It follows that $3^{k+1} - 2$ is even, which is what we needed to show."

ANSWERS FOR TEST YOURSELF

1. deductive **2.** prove

5.4 Strong Mathematical Induction and the Well-Ordering Principle for the Integers

Mathematics takes us still further from what is human into the region of absolute necessity, to which not only the actual world, but every possible world, must conform.
—Bertrand Russell, 1902

Strong mathematical induction is similar to ordinary mathematical induction in that it is a technique for establishing the truth of a sequence of statements about integers. Also, a proof by strong mathematical induction consists of a basis step and an inductive step. However, the basis step may contain proofs for several initial values, and in the inductive step the truth of the predicate $P(n)$ is assumed not just for one value of n but for *all* values through k, and then the truth of $P(k + 1)$ is proved.

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a)$, $P(a + 1)$, . . . , and $P(b)$ are all true. **(basis step)**
2. For every integer $k \geq b$, if $P(i)$ is true for each integer i from a through k, then $P(k + 1)$ is true. **(inductive step)**

Then the statement

$$\text{for every integer } n \geq a,\ P(n)$$

is true. (The supposition that $P(i)$ is true for each integer i from a through k is called the **inductive hypothesis**. Another way to state the inductive hypothesis is to say that $P(a)$, $P(a + 1)$, . . . , $P(k)$ are all true.)

Any statement that can be proved with ordinary mathematical induction can be proved with strong mathematical induction. The reason is that given any integer $k \geq b$, if the truth of $P(k)$ alone implies the truth of $P(k + 1)$, then certainly the truth of $P(a)$, $P(a + 1)$, . . . , and $P(k)$ implies the truth of $P(k + 1)$. It is also the case that any statement that can be proved with strong mathematical induction can be proved with ordinary mathematical induction. A proof is sketched in exercise 27 at the end of this section.

Strictly speaking, the principle of strong mathematical induction can be written without a basis step if the inductive step is changed to "For every integer $k \geq a - 1$, if $P(i)$ is true for each integer i from a through k, then $P(k + 1)$ is true." The reason for this is that the statement "$P(i)$ is true for each integer i from a through k" is vacuously true for $k = a - 1$. Hence, if the implication in the inductive step is true, then the conclusion $P(a)$ must also

be true,* which proves the basis step. However, in many cases the proof of the implication for $k > b$ does not work for $a \leq k \leq b$. So it is a good idea to get into the habit of thinking separately about the cases where $a \leq k \leq b$ by explicitly including a basis step.

The principle of strong mathematical induction is known under a variety of different names including the *second principle of induction*, the *second principle of finite induction*, and the *principle of complete induction*.

Applying Strong Mathematical Induction

The divisibility-by-a-prime theorem states that any integer greater than 1 is divisible by a prime number. We prove this theorem using strong mathematical induction.

Example 5.4.1 **Divisibility by a Prime**

Prove Theorem 4.4.4: Any integer greater than 1 is divisible by a prime number.

Solution The idea for the inductive step is this: If you are given an integer greater than 1 that is not itself prime, then it is a product of two smaller positive integers, each of which is greater than 1. By inductive hypothesis, you are assuming that each of these smaller integers is divisible by a prime number, and so, by transitivity of divisibility, those prime numbers also divide the integer you started with.

Proof (by strong mathematical induction):

Let the property $P(n)$ be the sentence

n is divisible by a prime number. ← $P(n)$

Show that P(2) is true:
To establish $P(2)$, we must show that

2 is divisible by a prime number. ← $P(2)$

But this is true because 2 is divisible by 2 and 2 is a prime number.

Show that for every integer k ≥ 2, if P(i) is true for each integer from 2 through k, then P(k + 1) is also true:
Let k be any integer with $k \geq 2$ and suppose that

i is divisible by a prime number for each integer i from 2 through k. ← inductive hypothesis

We must show that

$k + 1$ is divisible by a prime number. ← $P(k + 1)$

Case 1 (k + 1 is prime): In this case $k + 1$ is divisible by a prime number, namely, itself.

Case 2 (k + 1 is not prime): In this case $k + 1 = ab$ where a and b are integers with $1 < a < k + 1$ and $1 < b < k + 1$. Thus, in particular, $2 \leq a \leq k$, and so by inductive hypothesis, a is divisible by a prime number p. In addition because $k + 1 = ab$, we have that $k + 1$ is divisible by a. Hence, since $k + 1$ is divisible by a and a is divisible by p, by transitivity of divisibility, $k + 1$ is divisible by the prime number p.

*If you have proved that a certain if-then statement is true and if you also know that the hypothesis is true, then the conclusion must be true.

Therefore, regardless of whether $k+1$ is prime or not, it is divisible by a prime number *[as was to be shown].*
[Since we have proved both the basis and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]

■

Both ordinary and strong mathematical induction can be used to show that the terms of certain sequences satisfy certain properties. The next example shows how this is done using strong induction.

Example 5.4.2 **Proving a Property of a Sequence with Strong Induction**

Define a sequence $s_0, s_1, s_2, \ldots$ as follows:

$$s_0 = 0, \quad s_1 = 4, \quad s_k = 6a_{k-1} - 5a_{k-2} \quad \text{for every integer } k \geq 2.$$

a. Find the first four terms of this sequence.

b. It is claimed that for each integer $n \geq 0$, the nth term of the sequence has the same value as that given by the formula $5^n - 1$. In other words, the claim is that all the terms of the sequence satisfy the equation $s_n = 5^n - 1$. Prove that this is true.

Solution

a. $s_0 = 0, \quad s_1 = 4, \quad s_2 = 6s_1 - 5s_0 = 6 \cdot 4 - 5 \cdot 0 = 24,$
$s_3 = 6s_2 - 5s_1 = 6 \cdot 24 - 5 \cdot 4 = 144 - 20 = 124$

b. To use strong mathematical induction to show that every term of the sequence satisfies the equation, the basis step must show that the first two terms satisfy it. This is necessary because, according to the definition of the sequence, computing values of later terms requires knowing the values of the *two* previous terms. So if the basis step only shows that the first term satisfies the equation, it would not be possible to use the inductive step to deduce that the second term satisfies the equation. In the inductive step you suppose that for an arbitrarily chosen integer $k \geq 1$, all the terms of the sequence from s_0 through s_k satisfy the given equation and you then deduce that s_{k+1} must also satisfy the equation.

Proof:

Let $s_0, s_1, s_2, \ldots$ be the sequence defined by specifying that $s_0 = 0$, $s_1 = 4$, and $s_k = 6a_{k-1} - 5a_{k-2}$ for every integer $k \geq 2$, and let the property $P(n)$ be the formula

$$s_n = 5^n - 1. \qquad \leftarrow P(n)$$

We will use strong mathematical induction to prove that for every integer $n \geq 0$, $P(n)$ is true.

Show that P(0) and P(1) are true:
To establish $P(0)$ and $P(1)$, we must show that

$$s_0 = 5^0 - 1 \text{ and } s_1 = 5^1 - 1. \qquad \leftarrow P(0) \text{ and } P(1)$$

But, by definition of $s_0, s_1, s_2, \ldots$, we have that $s_0 = 0$ and $s_1 = 4$. Since $5^0 - 1 = 1 - 1 = 0$ and $5^1 - 1 = 5 - 1 = 4$, the values of s_0 and s_1 agree with the values given by the formula.

(continued on page 304)

Show that for every integer $k \geq 1$, if $P(i)$ is true for each integer i from 0 through k, then $P(k+1)$ is also true:
Let k be any integer with $k \geq 1$ and suppose that

$$s_i = 5^i - 1 \text{ for each integer } i \text{ with } 0 \leq i \leq k. \qquad \leftarrow \text{inductive hypothesis}$$

We must show that

$$s_{k+1} = 5^{k+1} - 1. \qquad \leftarrow P(k+1)$$

But since $k \geq 1$, we have that $k + 1 \geq 2$, and so

$$\begin{aligned}
s_{k+1} &= 6s_k - 5s_{k-1} && \text{by definition of } s_0, s_1, s_2, \ldots \\
&= 6(5^k - 1) - 5(5^{k-1} - 1) && \text{by definition hypothesis} \\
&= 6 \cdot 5^k - 6 - 5^k + 5 && \text{by multiplying out and applying a law of exponents} \\
&= (6-1)5^k - 1 && \text{by factoring out 6 and arithmetic} \\
&= 5 \cdot 5^k - 1 && \text{by arithmetic} \\
&= 5^{k+1} - 1 && \text{by applying a law of exponents,}
\end{aligned}$$

[as was to be shown].
[Since we have proved both the basis and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]

■

Example 5.4.3 **A Sequence That Involves the Floor Function**

Define a sequence $a_1, a_2, a_3, \ldots$ as follows:

$$\begin{aligned}
a_1 &= 0, \\
a_2 &= 2, \\
a_k &= 3a_{\lfloor k/2 \rfloor} + 2 \quad \text{for each integer } k \geq 3.
\end{aligned}$$

a. Find the first seven terms of the sequence.

b. Prove that a_n is even for every integer $n \geq 1$.

Solution

a. $a_1 = 0$
$a_2 = 2$
$a_3 = 3a_{\lfloor 3/2 \rfloor} + 2 = 3a_1 + 2 = 3 \cdot 0 + 2 = 2$
$a_4 = 3a_{\lfloor 4/2 \rfloor} + 2 = 3a_2 + 2 = 3 \cdot 2 + 2 = 8$
$a_5 = 3a_{\lfloor 5/2 \rfloor} + 2 = 3a_2 + 2 = 3 \cdot 2 + 2 = 8$
$a_6 = 3a_{\lfloor 6/2 \rfloor} + 2 = 3a_3 + 2 = 3 \cdot 2 + 2 = 8$
$a_7 = 3a_{\lfloor 7/2 \rfloor} + 2 = 3a_3 + 2 = 3 \cdot 2 + 2 = 8$

b. Let the property $P(n)$ be the sentence "a_n is even." We use strong mathematical induction to show that the property holds for every integer $n \geq 1$.

Show that $P(1)$ and $P(2)$ are true: The property is true for $n = 1$ and $n = 2$ because $a_1 = 0$ and $a_2 = 2$ and both 0 and 2 are even integers.

Show that for every integer $k \geq 1$, if $P(i)$ is true for each integer i from 1 through k, then $P(k+1)$ is also true: Let k be any integer with $k \geq 1$ and suppose that

$$a_i \text{ is even for each integer } i \text{ with } 1 \leq i \leq k. \qquad \leftarrow \text{inductive hypothesis}$$

[We must show that a_k is even.] By definition of $a_1, a_2, a_3, \ldots$

$$a_k = 3a_{\lfloor k/2 \rfloor} + 2 \quad \text{for every integer } k \geq 3. \qquad \leftarrow P(k+1)$$

Now $a_{\lfloor k/2 \rfloor}$ is even by the inductive hypothesis *[because $k \geq 1$ and so $1 \leq \lfloor k/2 \rfloor \leq k$]*. Thus $3a_{\lfloor k/2 \rfloor}$ is even *[because it is a product of an odd and an even integer]*, and hence $3a_{\lfloor k/2 \rfloor} + 2$ is even *[because a sum of two even integers is even]*. Consequently, a_k, which equals $3a_{\lfloor k/2 \rfloor} + 2$, is even *[as was to be shown]*.

[Since we have proved the basis step and the inductive step of the strong mathematical induction, we conclude that the given statement is true.] ■

Another use of strong induction concerns the computation of products. A product of four numbers may be computed in a variety of different ways as indicated by the placement of parentheses. For instance,

$((x_1x_2)x_3)x_4$ means multiply x_1 and x_2, multiply the result by x_3, and then multiply that number by x_4,

and

$(x_1x_2)(x_3x_4)$ means multiply x_1 and x_2, multiply x_3 and x_4, and then take the product of the two.

Note that in both examples above, although the factors are multiplied in a different order, the number of multiplications—three—is the same. Strong mathematical induction is used to prove a generalization of this fact.

Note Like many definitions, this may look strange but it makes things work out nicely for extreme cases.

Convention

Let us agree to say that a single number x_1 is a product with one factor and can be computed with zero multiplications.

Example 5.4.4 **The Number of Multiplications Needed to Multiply *n* Numbers**

Prove that for any integer $n \geq 1$, if $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

Solution The truth of the basis step follows immediately from the convention about a product with one factor. The inductive step is based on the fact that when several numbers are multiplied together, each step of the process involves multiplying two individual quantities. For instance, the final step for computing $((x_1x_2)x_3)(x_4x_5)$ is to multiply $(x_1x_2)x_3$ and x_4x_5. In general, when $k+1$ numbers are multiplied, the two quantities in the final step each consist of fewer than $k+1$ factors. This is what makes it possible to use the inductive hypothesis.

Proof (by strong mathematical induction):

Let the property $P(n)$ be the sentence

> If $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$. ← $P(n)$

Show that P(1) is true:
To establish $P(1)$, we must show that

> The number of multiplications needed to compute the product of x_1 is $1 - 1$. ← $P(1)$

This is true because, by convention, x_1 is a product that can be computed with 0 multiplications, and $0 = 1 - 1$.

Show that for every integer $k \geq 1$, if P(i) is true for each integer i from 1 through k, then P(k + 1) is also true:
Let k be any integer with $k \geq 1$ and suppose that

> For each integer i from 1 through k, if $x_1, x_2, \ldots, x_i$ are numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $i - 1$. ← inductive hypothesis

We must show that

> If $x_1, x_2, \ldots, x_{k+1}$ are $k + 1$ numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $(k + 1) - 1 = k$. ← $P(k + 1)$

Consider a product of $k + 1$ factors: $x_1, x_2 \ldots, x_{k+1}$. When parentheses are inserted in order to compute the product, some multiplication is the final one and each of the two factors making up the final multiplication is a product of fewer than $k + 1$ factors. Let L be the product of the left-hand factors and R be the product of the right-hand factors, and suppose that L is composed of l factors and R is composed of r factors. Then $l + r = k + 1$, the total number of factors in the product, and

$$1 \leq l \leq k \quad \text{and} \quad 1 \leq r \leq k.$$

By inductive hypothesis, evaluating L takes $l - 1$ multiplications and evaluating R takes $r - 1$ multiplications. Because one final multiplication is needed to evaluate $L \cdot R$, the number of multiplications needed to evaluate the product of all $k + 1$ factors is

$$(l - 1) + (r - 1) + 1 = (l + r) - 1 = (k + 1) - 1 = k$$

[as was to be shown].
[Since we have proved the basis step and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]

■

Strong mathematical induction makes possible a proof of the fact used frequently in computer science that every positive integer n has a unique binary integer representation. The proof looks complicated because of all the notation needed to write down the various steps.

But the idea of the proof is simple. It is that if integers smaller than n have unique representations as sums of powers of 2, then the unique representation for n as a sum of powers of 2 can be found by taking the representation for $n/2$ (or for $(n-1)/2$ if n is odd) and multiplying it by 2.

Theorem 5.4.1 Existence and Uniqueness of Binary Integer Representations

Given any positive integer n, n has a unique representation in the form

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for each $j = 0, 1, 2, \ldots, r-1$.

Proof:

We give separate proofs by strong mathematical induction to show first the existence and second the uniqueness of the binary representation.

Existence (proof by strong mathematical induction): Let the property $P(n)$ be the equation

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0, \qquad \leftarrow P(n)$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for each $j = 0, 1, 2, \ldots, r-1$.

Show that P(1) is true:

Let $r = 0$ and $c_0 = 1$. Then $1 = c_r \cdot 2^r$, and so $n = 1$ can be written in the required form.

Show that for every integer $k \geq 1$, if $P(i)$ is true for each integer i from 1 through k, then $P(k+1)$ is also true:

Let k be an integer with $k \geq 1$. Suppose that for each integer i from 1 through k,

$$i = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0, \qquad \leftarrow \text{inductive hypothesis}$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for each $j = 0, 1, 2, \ldots, r-1$. We must show that $k+1$ can be written as a sum of powers of 2 in the required form.

Case 1 ($k+1$ is even): In this case $(k+1)/2$ is an integer, and by inductive hypothesis, since $1 \leq (k+1)/2 \leq k$, then

$$\frac{k+1}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for each $j = 0, 1, 2, \ldots, r-1$. Multiplying both sides of the equation by 2 gives

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2,$$

which is a sum of powers of 2 of the required form.

Case 2 ($k+1$ is odd): In this case $k/2$ is an integer, and by inductive hypothesis, since $1 \leq k/2 = k$, then

$$\frac{k}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

(continued on page 308)

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for each $j = 0, 1, 2, \ldots, r-1$. Multiplying both sides of the equation by 2 and adding 1 gives

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2 + 1,$$

which is also a sum of powers of 2 of the required form.

The preceding arguments show that regardless of whether $k+1$ is even or odd, $k+1$ has a representation of the required form. *[Or, in other words, $P(k+1)$ is true as was to be shown.]*

[Since we have proved the basis step and the inductive step of the strong mathematical induction, the existence half of the theorem is true.]

Uniqueness: To prove uniqueness, suppose that there is an integer n with two different representations as a sum of nonnegative integer powers of 2. Equating the two representations and canceling all identical terms gives

$$2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 = 2^s + d_{s-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0 \qquad 5.4.1$$

where r and s are nonnegative integers and each c_i and each d_i equal 0 or 1. Without loss of generality, we may assume that $r < s$. Now by the formula for the sum of a geometric sequence (Theorem 5.2.2) and because $r < s$ (which implies that $r+1 \leq s$),

$$\begin{aligned} 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 &\leq 2^r + 2^{r-1} + \cdots + 2 + 1 = 2^{r+1} - 1 \\ &< 2^s. \end{aligned}$$

Thus

$$2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 < 2^s + d_{s-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0,$$

which contradicts equation (5.4.1). Hence the supposition is false, so any integer n has only one representation as a sum of nonnegative integer powers of 2.

The Well-Ordering Principle for the Integers

The well-ordering principle for the integers looks very different from both the ordinary and the strong principles of mathematical induction, but it can be shown that all three principles are equivalent. In other words, if any one of the three is true, then so are both of the others.

Well-Ordering Principle for the Integers

Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

When the context makes the reference clear, we will write simply "the well-ordering principle" rather than "the well-ordering principle for the integers."

Example 5.4.5 **Finding Least Elements**

In each case, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

a. The set of all positive real numbers

b. The set of all nonnegative integers n such that $n^2 < n$

c. The set of all nonnegative integers of the form $46 - 7k$, where k is an integer

Solution

a. There is no least positive real number. For if x is any positive real number, then $x/2$ is a positive real number that is less than x. No violation of the well-ordering principle occurs because the well-ordering principle refers only to sets of integers, and this set is not a set of integers.

b. There is no *least* nonnegative integer n such that $n^2 < n$ because there is *no* nonnegative integer that satisfies this inequality. The well-ordering principle is not violated because the well-ordering principle refers only to sets that contain at least one element.

c. The following table shows values of $46 - 7k$ for various values of k.

k	0	1	2	3	4	5	6	7	⋯	−1	−2	−3	⋯
$46 - 7k$	46	39	32	25	18	11	4	−3	⋯	53	60	67	⋯

The table suggests, and you can easily confirm, that $46 - 7k < 0$ for $k \geq 7$ and that $46 - 7k \geq 46$ for $k \leq 0$. Therefore, from the other values in the table it is clear that 4 is the least nonnegative integer of the form $46 - 7k$. This corresponds to $k = 6$. ■

Another way to look at the analysis of Example 5.4.5(c) is to observe that subtracting six 7's from 46 leaves 4 left over and this is the least nonnegative integer obtained by repeated subtraction of 7's from 46. In other words, 6 is the quotient and 4 is the remainder for the division of 46 by 7. More generally, in the division of any integer n by any positive integer d, the remainder r is the least nonnegative integer of the form $n - dk$. This is the heart of the following proof of the existence part of the quotient-remainder theorem (the part that guarantees the existence of a quotient and a remainder of the division of an integer by a positive integer). For a proof of the uniqueness of the quotient and remainder, see exercise 21 of Section 4.8.

Quotient-Remainder Theorem (Existence Part)

Given any integer n and any positive integer d, there exist integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Proof: Let S be the set of all nonnegative integers of the form

$$n - dk,$$

where k is an integer. This set has at least one element. *[For if n is nonnegative, then*

$$n - 0 \cdot d = n \geq 0,$$

and so $n - 0 \cdot d$ is in S. And if n is negative, then

$$n - nd = \underbrace{n}_{< 0}\underbrace{(1 - d)}_{\leq 0 \text{ since } d \text{ is a positive integer}} \geq 0,$$

(continued on page 310)

and so $n - nd$ is in S.] It follows by the well-ordering principle for the integers that S contains a least element r. Then, for some specific integer value of k, say q,

$$n - dq = r$$

[because every integer in S can be written in this form]. Adding dq to both sides gives

$$n = dq + r.$$

Furthermore, $r < d$. *[For suppose $r \geq d$. Then*

$$n - d(q + 1) = n - dq - d = r - d \geq 0,$$

and so $n - d(q + 1)$ would be a nonnegative integer in S that would be smaller than r. But r is the smallest integer in S. This contradiction shows that the supposition $r \geq d$ must be false.] The preceding arguments prove that there exist integers r and q for which

$$n = dq + r \quad \text{and} \quad 0 \leq r < d$$

[as was to be shown].

Another consequence of the well-ordering principle is the fact that any strictly decreasing sequence of nonnegative integers is finite. That is, if $r_1, r_2, r_3, \ldots$ is a sequence of nonnegative integers satisfying

$$r_i > r_{i+1}$$

for every $i \geq 1$, then $r_1, r_2, r_3, \ldots$ is a finite sequence. *[For by the well-ordering principle such a sequence has a least element, say r_k. It follows that r_k is the final term of the sequence because if there were an additional term r_{k+1}, then since the sequence is strictly decreasing, $r_{k+1} < r_k$, which would be a contradiction.]* This fact is frequently used in computer science to prove that algorithms terminate after a finite number of steps.

TEST YOURSELF

1. In a proof by strong mathematical induction the basis step may require checking a property $P(n)$ for more _____ value of n.
2. Suppose that in the basis step for a proof by strong mathematical induction the property $P(n)$ was checked for every integer n from a through b. Then in the inductive step one assumes that for any integer $k \geq b$, the property $P(n)$ is true for all values of i from _____ through _____ and one shows that _____ is true.
3. According to the well-ordering principle for the integers, if a set S of integers contains at least _____ and if there is some integer that is less than or equal to every _____, then _____.

EXERCISE SET 5.4

1. Suppose $a_1, a_2, a_3, \ldots$ is a sequence defined as follows:

   $a_1 = 1, \ a_2 = 3,$

   $a_k = a_{k-2} + 2a_{k-1}$ for each integer $k \geq 3$.

   Prove that a_n is odd for every integer $n \geq 1$.

2. Suppose $b_1, b_2, b_3, \ldots$ is a sequence defined as follows:

   $b_1 = 4, \ b_2 = 12,$

   $b_k = b_{k-2} + b_{k-1}$ for each integer $k \geq 3$.

   Prove that b_n is divisible by 4 for every integer $n \geq 1$.

3. Suppose that $c_0, c_1, c_2, \ldots$ is a sequence defined as follows:

$$c_0 = 2,\ c_1 = 2,\ c_2 = 6,$$
$$c_k = 3c_{k-3} \quad \text{for every integer } k \geq 3.$$

Prove that c_n is even for each integer $n \geq 0$.

4. Suppose that $d_1, d_2, d_3, \ldots$ is a sequence defined as follows:

$$d_1 = \frac{9}{10},\ d_2\frac{10}{11},$$
$$d_k = d_{k-1} \cdot d_{k-2} \quad \text{for every integer } k \geq 3.$$

Prove that $0 < d_n \leq 1$ for each integer $n \geq 1$.

5. Suppose that $e_0, e_1, e_2, \ldots$ is a sequence defined as follows:

$$e_0 = 12,\ e_1 = 29,$$
$$e_k = 5e_{k-1} - 6e_{k-2} \quad \text{for each integer } k \geq 2.$$

Prove that $e_n = 5 \cdot 3^n + 7 \cdot 2^n$ for every integer $n \geq 0$.

6. Suppose that $f_0, f_1, f_2, \ldots$ is a sequence defined as follows:

$$f_0 = 5,\ f_1 = 16,$$
$$f_k = 7f_{k-1} - 10f_{k-2} \quad \text{for every integer } k \geq 2.$$

Prove that $f_n = 3 \cdot 2^n + 2 \cdot 5^n$ for each integer $n \geq 0$.

7. Suppose that $g_1, g_2, g_3, \ldots$ is a sequence defined as follows:

$$g_1 = 3,\ g_2 = 5,$$
$$g_k = 3g_{k-1} - 2g_{k-2} \quad \text{for each integer } k \geq 3.$$

Prove that $g_n = 2^n + 1$ for every integer $n \geq 1$.

8. Suppose that $h_0, h_1, h_2, \ldots$ is a sequence defined as follows:

$$h_0 = 1,\ h_1 = 2,\ h_2 = 3,$$
$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{for each integer } k \geq 3.$$

a. Prove that $h_n \leq 3^n$ for every integer $n \geq 0$.

b. Suppose that s is any real number such that $s^3 \geq s^2 + s + 1$. (This implies that $2 > s > 1.83$.) Prove that $h_n \leq s^n$ for every integer $n \geq 2$.

9. Define a sequence $a_1, a_2, a_3, \ldots$ as follows: $a_1 = 1$, $a_2 = 3$, and $a_k = a_{k-1} + a_{k-2}$ for every integer $k \geq 3$. (This sequence is known as the Lucas sequence.) Use strong mathematical induction to prove that $a_n \leq \left(\frac{7}{4}\right)^n$ for every integer $n \geq 1$.

***H* 10.** The introductory example solved with ordinary mathematical induction in Section 5.3 can also be solved using strong mathematical induction. Let $P(n)$ be "any $n¢$ can be obtained using a combination of $3¢$ and $5¢$ coins." Use strong mathematical induction to prove that $P(n)$ is true for every integer $n \geq 8$.

11. You begin solving a jigsaw puzzle by finding two pieces that match and fitting them together. Every subsequent step of the solution consists of fitting together two blocks, each of which is made up of one or more pieces that have previously been assembled. Use strong mathematical induction to prove that for every integer $n \geq 1$, the number of steps required to put together all n pieces of a jigsaw puzzle is $n - 1$.

***H* 12.** The sides of a circular track contain a sequence of n cans of gasoline. For each integer $n \geq 1$, the total amount in the cans is sufficient to enable a certain car to make one complete circuit of the track. In addition, all the gasoline could fit into the car's gas tank at one time. Use mathematical induction to prove that it is possible to find an initial location for placing the car so that it will be able to traverse the entire track by using the various amounts of gasoline in the cans that it encounters along the way.

***H* 13.** Use strong mathematical induction to prove the existence part of the unique factorization of integers theorem (Theorem 4.4.5). In other words, prove that every integer greater than 1 is either a prime number or a product of prime numbers.

14. Any product of two or more integers is a result of successive multiplications of two integers at a time. For instance, here are a few of the ways in which $a_1a_2a_3a_4$ might be computed: $(a_1a_2)(a_3a_4)$ or $((a_1a_2)a_3)a_4)$ or $a_1((a_2a_3)a_4)$. Use strong mathematical induction to prove that any product of two or more odd integers is odd.

15. Define the "sum" of one integer to be that integer, and use strong mathematical induction to prove that for every integer $n \geq 1$, any sum of n even integers is even.

***H* 16.** Use strong mathematical induction to prove that for every integer $n \geq 2$, if n is even, then any sum

of n odd integers is even, and if n is odd, then any sum of n odd integers is odd.

17. Compute 4^1, 4^2, 4^3, 4^4, 4^5, 4^6, 4^7, and 4^8. Make a conjecture about the units digit of 4^n where n is a positive integer. Use strong mathematical induction to prove your conjecture.

18. Compute 9^0, 9^1, 9^2, 9^3, 9^4, and 9^5. Make a conjecture about the units digit of 9^n where n is a positive integer. Use strong mathematical induction to prove your conjecture.

19. Suppose that $a_1, a_2, a_3, \ldots$ is a sequence defined as follows:

$a_1 = 1$ $a_k = 2 \cdot a_{\lfloor k/2 \rfloor}$ for every integer $k \geq 2$.

Prove that $a_n \leq n$ for each integer $n \geq 1$.

20. Suppose that $b_1, b_2, b_3, \ldots$ is a sequence defined as follows:

$b_1 = 0$, $b_2 = 3$ $b_k = 5 \cdot b_{\lfloor k/2 \rfloor} + 6$ for every integer $k \geq 3$.

Prove that b_n is divisible by 3 for each integer $n \geq 1$.

21. Suppose that $c_1, c_2, c_3, \ldots$ is a sequence defined as follows:

$c_0 = 1$, $c_1 = 1$ $c_k = c_{\lfloor k/2 \rfloor} + c_{\lfloor k/2 \rfloor}$ for every integer $k \geq 2$.

Prove that $c_n = n$ for each integer $n \geq 1$.

22. One version of the game NIM starts with two piles of objects such as coins, stones, or matchsticks. In each turn a player is required to remove from one to three objects from one of the piles. The two players take turns doing this until both piles are empty. The loser is the first player who can't make a move. Use strong mathematical induction to show that if both piles contain the same number of objects at the start of the game, the player who goes second can always win.

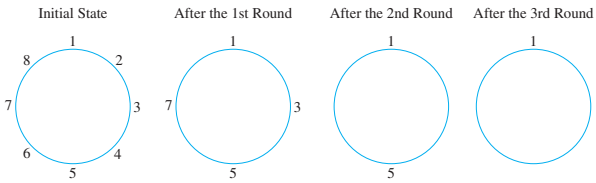
23. Define a game G as follows: Begin with a pile of n stones and 0 points. In the first move split the pile into two possibly unequal sub-piles, multiply the number of stones in one sub-pile times the number of stones in the other sub-pile, and add the product to your score. In the second move, split each of the newly created piles into a pair of possibly unequal sub-piles, multiply the number of stones in each sub-pile times the number of stones in the paired sub-pile, and add the new products to your score. Continue by successively splitting each newly created pile of stones that has at least two stones into a pair of sub-piles, multiplying the number of stones in each sub-pile times the number of stones in the paired sub-pile, and adding the new products to your score. The game G ends when no pile contains more than one stone.

a. Play G starting with 10 stones and using the following initial moves. In move 1 split the pile of 10 stones into two sub-piles with 3 and 7 stones respectively, compute $3 \cdot 7 = 21$, and find that your score is 21. In move 2 split the pile of 3 stones into two sub-piles, with 1 and 2 stones respectively, and split the pile of 7 stones into two sub-piles, with 4 and 3 stones respectively, compute $1 \cdot 2 = 2$ and $4 \cdot 3 = 12$, and find that your score is $21 + 2 + 12 = 35$. In move 3 split the pile of 4 stones into two sub-piles, each with 2 stones, and split the pile of 3 stones into two sub-piles, with 1 and 2 stones respectively, and find your new score. Continue splitting piles and computing your score until no pile has more than one stone. Show your final score along with a record of the numbers of stones in the piles you created with your moves.

b. Play G again starting with 10 stones, but use a different initial move from the one in part (a). Show your final score along with a record of the numbers of stones in the piles you created with your moves.

c. Show that you can use strong mathematical induction to prove that for every integer $n \geq 1$, given the set-up of game G, no matter how you split the piles in the various moves, your final score is $(n(n-1))/2$. The basis step may look a little strange because a pile consisting of one stone cannot be spilt into any sub-piles. Another way to say this is that it can only be split into zero piles, and that gives an answer that agrees with the general formula for the final score.

24. Imagine a situation in which eight people, numbered consecutively 1–8, are arranged in a circle. Starting from person #1, every second person in the circle is eliminated. The elimination process continues until only one person remains. In the first round the people numbered 2, 4, 6, and 8 are eliminated, in the second round the people numbered 3 and 7 are eliminated, and in the third round person #5 is eliminated, so after the third round only person #1 remains, as shown on the next page.



a. Given a set of sixteen people arranged in a circle and numbered, consecutively 1–16, list the numbers of the people who are eliminated in each round if every second person is eliminated and the elimination process continues until only one person remains. Assume that the starting point is person #1.

b. Use ordinary mathematical induction to prove that for every integer $n \geq 1$, given any set of 2^n people arranged in a circle and numbered consecutively 1 through 2^n, if one starts from person #1 and goes repeatedly around the circle successively eliminating every second person, eventually only person #1 will remain.

c. Use the result of part (b) to prove that for any nonnegative integers n and m with $2^n \leq 2^n + m < 2^{n+1}$, if $r = 2^n + m$, then given any set of r people arranged in a circle and numbered consecutively 1 through r, if one starts from person #1 and goes repeatedly around the circle successively eliminating every second person, eventually only person #$(2m + 1)$ will remain.

25. Find the mistake in the following "proof" that purports to show that every nonnegative integer power of every nonzero real number is 1.

"**Proof:** Let r be any nonzero real number and let the property $P(n)$ be the equation $r^n = 1$.

Show that P(0) is true: $P(0)$ is true because $r^0 = 1$ by definition of zeroth power.

Show that for every integer k ≥ 0, if P(i) is true for each integer i from 0 through k, then P(k + 1) is also true: Let k be any integer with $k \geq 0$ and suppose that $r^i = 1$ for each integer i from 0 through k. This is the inductive hypothesis. We must show that $r^{k+1} = 1$. Now

$$\begin{aligned} r^{k+1} &= r^{k+k-(k-1)} && \text{because } k+k-(k-1) = k+k-k+1 = k+1 \\ &= \frac{r^k \cdot r^k}{r^{k-1}} && \text{by the laws of exponents} \\ &= \frac{1 \cdot 1}{1} && \text{by inductive hypothesis} \\ &= 1. \end{aligned}$$

Thus $r^{k+1} = 1$ *[as was to be shown].*

[Since we have proved the basis step and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]"

26. Use the well-ordering principle for the integers to prove Theorem 4.4.4: Every integer greater than 1 is divisible by a prime number.

27. Use the well-ordering principle for the integers to prove the existence part of the unique factorization of integers theorem. In other words, prove that every integer greater than 1 is either prime or a product of prime numbers.

28. **a.** The Archimedean property for the rational numbers states that for every rational number r, there is an integer n such that $n > r$. Prove this property.

b. Prove that given any rational number r, the number $-r$ is also rational.

c. Use the results of parts (a) and (b) to prove that given any rational number r, there is an integer m such that $m < r$.

***H* 29.** Use the results of exercise 28 and the well-ordering principle for the integers to show that given any rational number r, there is an integer m such that $m \leq r < m + 1$.

30. Use the well-ordering principle to prove that given any integer $n \geq 1$, there exists an odd integer m and a nonnegative integer k such that $n = 2^k \cdot m$.

31. Give examples to illustrate the proof of Theorem 5.4.1.

32. Suppose $P(n)$ is a property such that

1. $P(0)$, $P(1)$, $P(2)$ are all true,
2. for each integer $k \geq 0$, if $P(k)$ is true, then $P(3k)$ is true. Must it follow that $P(n)$ is true for every integer $n \geq 0$? If yes, explain why; if no, give a counterexample.

33. Prove that if a statement can be proved by strong mathematical induction, then it can be proved by ordinary mathematical induction. To do this, let $P(n)$ be a property that is defined for each integer n, and suppose the following two statements are true:

1. $P(a), P(a + 1), P(a + 2), \ldots, P(b)$.
2. For any integer $k \geq b$, if $P(i)$ is true for each integer i from a through k, then $P(k + 1)$ is true.

The principle of strong mathematical induction would allow us to conclude immediately that $P(n)$

is true for every integer $n \geq a$. Can we reach the same conclusion using the principle of ordinary mathematical induction? Yes! To see this, let $Q(n)$ be the property

$P(j)$ is true for each integer j with $a \leq j \leq n$.

Then use ordinary mathematical induction to show that $Q(n)$ is true for every integer $n \geq b$. That is, prove:

1. $Q(b)$ is true.
2. For each integer $k \geq b$, if $Q(k)$ is true then $Q(k+1)$ is true.

H 34. It is a fact that every integer $n \geq 1$ can be written in the form

$$c_r \cdot 3^r + c_{r-1} \cdot 3^{r-1} + \cdots + c_2 \cdot 3^2 + c_1 \cdot 3 + c_0,$$

where $c_r = 1$ or 2 and $c_i = 0$, 1, or 2 for each integer $i = 0, 1, 2, \ldots, r-1$. Sketch a proof of this fact.

H* 35. Use mathematical induction to prove the existence part of the quotient-remainder theorem. In other words, use mathematical induction to prove that given any integer n and any positive integer d, there exist integers q and r such that $n = dq + r$ and $0 \leq r < d$.

H* 36. Prove that if a statement can be proved by ordinary mathematical induction, then it can be proved by the well-ordering principle.

H 37. Use the principle of ordinary mathematical induction to prove the well-ordering principle for the integers.

ANSWERS FOR TEST YOURSELF

1. than one **2.** a; k; $P(k+1)$ **3.** one integer; integer in S; S contains a least element

5.5 Application: Correctness of Algorithms

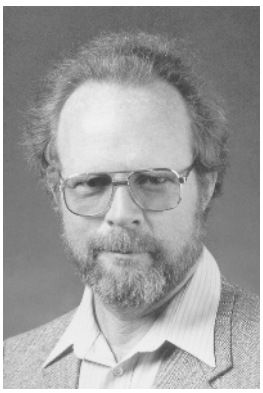
[P]rogramming reliably—must be an activity of an undeniably mathematical nature . . . . You see, mathematics is about thinking, and doing mathematics is always trying to think as well as possible. —Edsger W. Dijkstra (1981)

Edsger W. Dijkstra (1930–2002)

What does it mean for a computer program to be correct? Each program is designed to do a specific task—calculate the mean or median of a set of numbers, compute the size of the paychecks for a company payroll, rearrange names in alphabetical order, and so forth. We will say that a program is correct if it produces the output specified in its accompanying documentation for each set of input data of the type specified in the documentation.*

Most computer programmers write their programs using a combination of logical analysis and trial and error. In order to get a program to run at all, the programmer must first fix all syntax errors (such as writing **ik** instead of **if**, failing to declare a variable, or using a restricted keyword for a variable name). When the syntax errors have been removed, however, the program may still contain logical errors that prevent it from producing correct output. Frequently, programs are tested using sets of sample data for which the correct output is known in advance. And often the sample data are deliberately chosen to test the correctness of the program under extreme circumstances. But for most programs the number of possible sets of input data is either infinite or unmanageably large, and so no amount of program testing can give perfect confidence that the program will be correct for all possible sets of legal input data.

*Consumers of computer programs want an even more stringent definition of correctness. If a user puts in data of the wrong type, the user wants a decent error message, not a system crash.



Courtesy of Christiane Floyd

Robert W. Floyd (1936–2002)

Since 1967, with the publication of a paper by Robert W. Floyd,* considerable effort has gone into developing methods for proving programs correct at the time they are composed. One of the pioneers in this effort, Edsger W. Dijkstra, asserted that "we now take the position that it is not only the programmer's task to produce a correct program but also to demonstrate its correctness in a convincing manner."† Another leader in the field, David Gries, went so far as to say that "a program and its proof should be developed hand-in-hand, with the *proof* usually leading the way."** In this section we give an overview of the general format of correctness proofs and the details of one crucial technique, the *loop invariant procedure*, and we switch from using the term *program* to using the more general term *algorithm*.

Assertions

Consider an algorithm that is designed to produce a certain final state from a certain initial state. Both the initial and final states can be expressed as predicates involving the input and output variables. Often the predicate describing the initial state is called the **pre-condition for the algorithm**, and the predicate describing the final state is called the **post-condition for the algorithm**.

Example 5.5.1 **Algorithm Pre-Conditions and Post-Conditions**

Here are pre- and post-conditions for some typical algorithms.

a. Algorithm to compute a product of nonnegative integers

Pre-condition: The input variables m and n are nonnegative integers.

Post-condition: The output variable p equals mn.

b. Algorithm to find quotient and remainder of the division of one positive integer by another

Pre-condition: The input variables a and b are positive integers.

Post-condition: The output variables q and r are integers such that $a = bq + r$ and $0 \leq r < b$.

c. Algorithm to sort a one-dimensional array of real numbers

Pre-condition: The input variable $A[1], A[2], \ldots, A[n]$ is a one-dimensional array of real numbers.

Post-condition: The output variable $B[1], B[2], \ldots, B[n]$ is a one-dimensional array of real numbers with same elements as $A[1], A[2], \ldots, A[n]$ but with the property that $B[i] \leq B[j]$ whenever $i \leq j$. ■

A proof of algorithm correctness consists of showing that if the pre-condition for the algorithm is true for a collection of values for the input variables and if the statements of the algorithms are executed, then the post-condition is also true.

*R. W. Floyd, "Assigning meanings to programs," *Proc. Symp. Appl. Math.*, Amer. Math. Soc. **19** (1967), 19–32.

†Edsger Dijkstra in O. J. Dahl, E. W. Dijkstra, and C. A. R. Hoare, *Structured Programming* (London: Academic Press, 1972), p. 5.

**David Gries, *The Science of Programming* (New York: Springer-Verlag, 1981), p. 164.

The steps of an algorithm are divided into sections with assertions about the current state of algorithm variables inserted at strategically chosen points:

[*Assertion* 1*: pre-condition for the algorithm*]
{Algorithm statements}
[*Assertion* 2]
{Algorithm statements}
⋮
[*Assertion* $k-1$]
{Algorithm statements}
[*Assertion k: post-condition for the algorithm*]

Successive pairs of assertions are then treated as pre- and post-conditions for the algorithm statements between them. For each $i = 1, 2, \ldots, k-1$, one proves that if Assertion i is true and all the algorithm statements between Assertion i and Assertion $(i+1)$ are executed, then Assertion $(i+1)$ is true. Once all these individual proofs have been completed, one knows that Assertion k is true. And since Assertion 1 is the same as the pre-condition for the algorithm and Assertion k is the same as the post-condition for the algorithm, one concludes that the entire algorithm is correct with respect to its pre- and post-conditions.

Loop Invariants

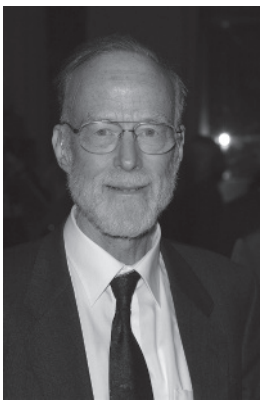
The method of loop invariants is used to prove correctness of a loop with respect to certain pre- and post-conditions. It is based on the principle of mathematical induction. Suppose that an algorithm contains a **while** loop and that entry to this loop is restricted by a condition G, called the **guard**. Suppose also that assertions describing the current states of algorithm variables have been placed immediately preceding and immediately following the loop. The assertion just preceding the loop is called the **pre-condition for the loop** and the one just following is called the **post-condition for the loop**. The annotated loop has the following appearance:

[*Pre-condition for the loop*]
while (G)
    [*Statements in the body of the loop.*
    None contain branching statements
    that lead outside the loop.]
end while
[*Post-condition for the loop*]

Definition

A loop is defined as **correct with respect to its pre- and post-conditions** if, and only if, whenever the algorithm variables satisfy the pre-condition for the loop and the loop terminates after a finite number of steps, the algorithm variables satisfy the post-condition for the loop.

Establishing the correctness of a loop uses the concept of loop invariant. A **loop invariant** is a predicate with domain a set of integers, which satisfies the following condition: For



R. Stonehouse/Camera Press/Redux

C. A. R. Hoare (born 1934)

each iteration of the loop, if the predicate is true before the iteration, then it is true after the iteration. Furthermore, if the predicate satisfies the following two additional conditions, the loop will be correct with respect to its pre- and post-conditions:

1. The predicate is true before the first iteration of the loop.
2. If the loop terminates after a finite number of iterations, the truth of the loop invariant ensures the truth of the post-condition for the loop.

The following theorem, called the *loop invariant theorem*, formalizes these ideas. It was first developed by C. A. R. Hoare in 1969.

Theorem 5.5.1 Loop Invariant Theorem

Let a **while** loop with guard G be given, together with pre- and post-conditions that are predicates in the algorithm variables. Also let a predicate $I(n)$, called the **loop invariant**, be given. If the following four properties are true, then the loop is correct with respect to its pre- and post-conditions.

I. Basis Property: The pre-condition for the loop implies that $I(0)$ is true before the first iteration of the loop.

II. Inductive Property: For every integer $k \geq 0$, if the guard G and the loop invariant $I(k)$ are both true before an iteration of the loop, then $I(k + 1)$ is true after an iteration of the loop.

III. Eventual Falsity of Guard: After a finite number of iterations of the loop, the guard G becomes false.

IV. Correctness of the Post-Condition: If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be as specified in the post-condition of the loop.

Proof: The loop invariant theorem follows easily from the principle of mathematical induction. Assume that $I(n)$ is a predicate that satisfies properties I–IV of the loop invariant theorem. *[We will prove that the loop is correct with respect to its pre- and post-conditions.]* Properties I and II are the basis and inductive steps needed to prove the truth of the following statement:

For every integer $n \geq 0$, if the **while** loop iterates n times, then $I(n)$ is true. 5.5.1

Thus, by the principle of mathematical induction, since both I and II are true, statement (5.5.1) is also true.

Property III says that the guard G eventually becomes false. At that point the loop will have been iterated some number, say N, of times. Since $I(n)$ is true after the nth iteration for every $n \geq 0$, then $I(n)$ is true after the Nth iteration. That is, after the Nth iteration the guard is false and $I(N)$ is true. But this is the hypothesis of property IV, which is an if-then statement. Since statement IV is true (by assumption) and its hypothesis is true (by the argument just given), it follows (by modus ponens) that its conclusion is also true. That is, the values of all algorithm variables after execution of the loop are as specified in the post-condition for the loop.

Developing a good loop invariant is a tricky process. Although learning how to do it is beyond the scope of this book, it is worth pursuing in a more advanced course.

Another tricky aspect of handling correctness proofs arises from the fact that execution of an algorithm is a dynamic process—it takes place in time. As execution progresses, the values of variables keep changing, yet often their names stay the same. In the following discussion, when we need to make a distinction between the values of a variable just before execution of an algorithm statement and just after execution of the statement, we will attach the subscripts *old* and *new* to the variable name.

Example 5.5.2 **Correctness of a Loop to Compute a Product**

The following loop is designed to compute the product mx for a nonnegative integer m and a real number x, without using a built-in multiplication operation. Prior to the loop, variables i and *product* have been introduced and given initial values $i = 0$ and $product = 0$.

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $product = 0$.]

while $(i \neq m)$

1. $product := product + x$
2. $i := i + 1$

end while

[Post-condition: $product = mx$]

Let the loop invariant be

$$I(n)\text{: } i = n \quad \text{and} \quad product = nx$$

The guard condition G of the **while** loop is

$$G\text{: } i \neq m$$

Use the loop invariant theorem to prove that the **while** loop is correct with respect to the given pre- and post-conditions.

Solution

I. Basis Property: *[$I(0)$ is true before the first iteration of the loop.]*

$I(0)$ is "$i = 0$ and $product = 0 \cdot x$," which is true before the first iteration of the loop because $0 \cdot x = 0$.

II. Inductive Property: *[If $G \wedge I(k)$ is true before a loop iteration (where $k \geq 0$), then $I(k + 1)$ is true after the loop iteration.]*

Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then as execution reaches the top of the loop, $i \neq m$, $product = kx$, and $i = k$. Since $i \neq m$, the guard is passed and statement 1 is executed. Before execution of statement 1,

$$\text{product}_{\text{old}} = kx.$$

Thus execution of statement 1 has the following effect:

$$\text{product}_{\text{new}} = \text{product}_{\text{old}} + x = kx + x = (k + 1)x.$$

Similarly, before statement 2 is executed,

$$i_{\text{old}} = k,$$

so after execution of statement 2,

$$i_{\text{new}} = i_{\text{old}} + 1 = k + 1.$$

Hence after the loop iteration, the statement $I(k+1)$, namely, ($i = k+1$ and $product = (k+1)x$), is true. This is what we needed to show.

III. Eventual Falsity of Guard: *[After a finite number of iterations of the loop, G becomes false.]*

The guard G is the condition $i \neq m$, and m is a nonnegative integer. By I and II, it is known that

> for every integer $n \geq 0$, if the loop is iterated n times, then $i = n$ and $product = nx$.

So after m iterations of the loop, $i = m$. Thus G becomes false after m iterations of the loop.

IV. Correctness of the Post-Condition: *[If N is the least number of iterations after which G is false and I(N) is true, then the value of the algorithm variables will be as specified in the post-condition of the loop.]*

According to the post-condition, the value of *product* after execution of the loop should be mx. But if G becomes false after N iterations, $i = m$. And if $I(N)$ is true, $i = N$ and $product = Nx$. Since both conditions (G false and $I(N)$ true) are satisfied, $m = i = N$ and $product = mx$ as required. ■

In the remainder of this section, we present proofs of the correctness of the crucial loops in the division algorithm and the Euclidean algorithm. (These algorithms were given in Section 4.10.)

Correctness of the Division Algorithm

The division algorithm is supposed to take a nonnegative integer a and a positive integer d and compute nonnegative integers q and r such that $a = dq + r$ and $0 \leq r < d$. Initially, the variables r and q are introduced and given the values $r = a$ and $q = 0$. The crucial loop, annotated with pre- and post-conditions, is the following:

[Pre-condition: a is a nonnegative integer and d is a positive integer, r = a, and q = 0.]

while $(r \geq d)$

1. $r := r - d$
2. $q := q + 1$

end while

[Post-condition: q and r are nonnegative integers with the property that $a = qd + r$ and $0 \leq r < d$.]

Proof:

To prove the correctness of the loop, let the loop invariant be

$$I(n)\text{: } r = a - nd \geq 0 \quad \text{and} \quad n = q.$$

The guard of the **while** loop is

$$G\text{: } r \geq d.$$

I. Basis Property: *[I(0) is true before the first iteration of the loop.]*

$I(0)$ is "$r = a - 0 \cdot d \geq 0$ and $q = 0$." But by the pre-condition, $r = a$, $a \geq 0$, and $q = 0$. So since $a = a - 0 \cdot d$, then $r = a - 0 \cdot d$ and $I(0)$ is true before the first iteration of the loop.

II. Inductive Property: *[If $G \wedge I(k)$ is true before an iteration of the loop (where $k \geq 0$), then $I(k+1)$ is true after iteration of the loop.]*

Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Since G is true, $r \geq d$ and the loop is entered. Also since $I(k)$ is true, $r = a - kd \geq 0$ and $k = q$. Hence, before execution of statements 1 and 2,

$$r_{\text{old}} \geq d \quad \text{and} \quad r_{\text{old}} = a - kd \quad \text{and} \quad q_{\text{old}} = k.$$

When statements 1 and 2 are executed, then

$$r_{\text{new}} = r_{\text{old}} - d = (a - kd) - d = a - (k+1)d \tag{5.5.2}$$

and

$$q_{\text{new}} = q_{\text{old}} + 1 = k + 1. \tag{5.5.3}$$

In addition, since $r_{\text{old}} \geq d$ before execution of statements 1 and 2, after execution of these statements,

$$r_{\text{new}} = r_{\text{old}} - d \geq d - d \geq 0. \tag{5.5.4}$$

Putting equations (5.5.2), (5.5.3), and (5.5.4) together shows that after iteration of the loop,

$$r_{\text{new}} \geq 0 \quad \text{and} \quad r_{\text{new}} = a - (k+1)d \quad \text{and} \quad q_{\text{new}} = k + 1.$$

Hence $I(k+1)$ is true.

III. Eventual Falsity of the Guard: *[After a finite number of iterations of the loop, G becomes false.]*

The guard G is the condition $r \geq d$. Each iteration of the loop reduces the value of r by d and yet leaves r nonnegative. Thus the values of r form a decreasing sequence of nonnegative integers, and so (by the well-ordering principle) there must be a smallest such r, say r_{min}. Then $r_{\text{min}} < d$. *[If r_{min} were greater than d, the loop would iterate another time, and a new value of r equal to $r_{\text{min}} - d$ would be obtained. But this new value would be smaller than r_{min}, which would contradict the fact that r_{min} is the smallest remainder obtained by repeated iteration of the loop.]* Hence as soon as the value $r = r_{\text{min}}$ is computed, the value of r becomes less than d, and so the guard G is false.

IV. Correctness of the Post-Condition: *[If N is the least number of iterations after which G is false and I(N) is true, then the values of the algorithm variables will be as specified in the post-condition of the loop.]*

Suppose that for some nonnegative integer N, G is false and $I(N)$ is true. Then $r < d$, $r = a - Nd$, $r \geq 0$, and $q = N$. Since $q = N$, substitution gives

$$r = a - qd,$$

and adding qd to both sides produces

$$a = qd + r.$$

Combining the two inequalities involving r gives

$$0 \leq r < d.$$

Because these are the values of q and r specified in the post-condition, the proof is complete. ■

Correctness of the Euclidean Theorem

The Euclidean algorithm is supposed to take integers A and B with $A > B \geq 0$ and compute their greatest common divisor. Just before the crucial loop, variables a, b, and r have been introduced with $a = A$, $b = B$, and $r = B$. The crucial loop, annotated with pre- and post-conditions, is the following:

[Pre-condition: A and B are integers with $A > B \geq 0$, $a = A$, $b = B$, $r = B$.]
while $(b \neq 0)$
1. $r := a \bmod b$
2. $a := b$
3. $b := r$

end while
[Post-condition: $a = \gcd(A, B)$.]

Proof:
To prove the correctness of the loop, let the invariant be

$$I(n)\text{: } \gcd(a, b) = \gcd(A, B) \quad \text{and} \quad 0 \leq b < a.$$

The guard of the **while** loop is

$$G\text{: } b \neq 0.$$

I. Basis Property: *[$I(0)$ is true before the first iteration of the loop.]*
$I(0)$ is

$$\gcd(A, B) = \gcd(a, b) \quad \text{and} \quad 0 \leq b < a.$$

According to the pre-condition,

$$a = A, \quad b = B, \quad r = B, \quad \text{and} \quad 0 \leq B < A.$$

Hence $\gcd(A, B) = \gcd(a, b)$. Since $0 \leq B < A$, $b = B$, and $a = A$ then $0 \leq b < a$. Hence $I(0)$ is true.

II. Inductive Property: *[If $G \wedge I(k)$ is true before an iteration of the loop (where $k \geq 0$), then $I(k + 1)$ is true after iteration of the loop.]*

Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. *[We must show that $I(k + 1)$ is true after iteration of the loop.]* Since G is true,

$b_{\text{old}} \neq 0$ and the loop is entered. And since $I(k)$ is true, immediately before statement 1 is executed,

$$\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(A, B) \quad \text{and} \quad 0 \leq b_{\text{old}} < a_{\text{old}}. \tag{5.5.5}$$

After execution of statement 1,

$$r_{\text{new}} = a_{\text{old}} \, mod \, b_{\text{old}}.$$

Thus, by the quotient-remainder theorem,

$$a_{\text{old}} = b_{\text{old}} \cdot q + r_{\text{new}} \quad \text{for some integer } q$$

and r_{new} has the property that

$$0 \leq r_{\text{new}} < b_{\text{old}}. \tag{5.5.6}$$

By Lemma 4.10.2,

$$\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(b_{\text{old}}, r_{\text{new}}).$$

So by the equation of (5.5.5),

$$\gcd(b_{\text{old}}, r_{\text{new}}) = \gcd(A, B). \tag{5.5.7}$$

When statements 2 and 3 are executed,

$$a_{\text{new}} = b_{\text{old}} \quad \text{and} \quad b_{\text{new}} = r_{\text{new}}. \tag{5.5.8}$$

Substituting equations (5.5.8) into equation (5.5.7) yields

$$\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(A, B). \tag{5.5.9}$$

And substituting the values from the equations in (5.5.8) into inequality (5.5.6) gives

$$0 \leq b_{\text{new}} < a_{\text{new}}. \tag{5.5.10}$$

Hence after the iteration of the loop, by equation (5.5.9) and inequality (5.5.10),

$$\gcd(a, b) = \gcd(A, B) \quad \text{and} \quad 0 \leq b < a,$$

which is $I(k+1)$. *[This is what we needed to show.]*

III. Eventual Falsity of the Guard: *[After a finite number of iterations of the loop, G becomes false.]*

Each value of b obtained by repeated iteration of the loop is nonnegative and less than the previous value of b. Thus, by the well-ordering principle, there is a least value b_{min}. The fact is that $b_{\text{min}} = 0$. *[If b_{min} is not 0, then the guard is true, and so the loop is iterated another time. In this iteration a value of r is calculated that is less than the previous value of b, b_{min}. Then the value of b is changed to r, which is less than b_{min}. This contradicts the fact that b_{min} is the least value of b obtained by repeated iteration of the loop. Hence $b_{\text{min}} = 0$.]* Since $b_{\text{min}} = 0$, the guard is false immediately following the loop iteration in which b_{min} is calculated.

IV. Correctness of the Post-Condition: *[If N is the least number of iterations after which G is false and I(N) is true, then the values of the algorithm variables will be as specified in the post-condition.]*

Suppose that for some nonnegative integer N, G is false and $I(N)$ is true. *[We must show the truth of the post-condition: $a = gcd(A, B)$.]* Since G is false, $b = 0$, and since $I(N)$ is true,

$$\gcd(a, b) = \gcd(A, B). \tag{5.5.11}$$

Substituting $b = 0$ into equation (5.5.11) gives

$$\gcd(a, 0) = \gcd(A, B).$$

But by Lemma 4.10.1,

$$\gcd(a, 0) = a.$$

Hence $a = \gcd(A, B)$ *[as was to be shown]*.

TEST YOURSELF

1. A pre-condition for an algorithm is _____ and a post-condition for an algorithm is _____.
2. A loop is defined as correct with respect to its pre- and post-conditions if, and only if, whenever the algorithm variables satisfy the pre-condition for the loop and the loop terminates after a finite number of steps, then _____.
3. For each iteration of a loop, if a loop invariant is true before iteration of the loop, then _____.
4. Given a **while** loop with guard G and a predicate $I(n)$ if the following four properties are true, then the loop is correct with respect to its pre- and post-conditions:

   (a) The pre-condition for the loop implies that _____ before the first iteration of the loop.
   (b) For every integer $k \geq 0$, if the guard G and the predicate $I(k)$ are both true before an iteration of the loop, then _____.
   (c) After a finite number of iterations of the loop, _____.
   (d) If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be as specified _____.

EXERCISE SET 5.5

Exercises 1–5 contain a while loop and a predicate. In each case show that if the predicate is true before entry to the loop, then it is also true after exit from the loop.

1. loop: **while** ($m \geq 0$ and $m \leq 100$)
   $m := m + 1$
   $n := n - 1$
   end while

   predicate: $m + n = 100$

2. loop: **while** ($m \geq 0$ and $m \leq 100$)
   $m := m + 4$
   $n := n - 2$
   end while

   predicate: $m + n$ is odd

3. loop: **while** ($m \geq 0$ and $m \leq 100$)
   $m := 3 \cdot m$
   $n := 5 \cdot n$
   end while

   predicate: $m^3 > n^2$

4. loop: **while** ($n \geq 0$ and $n \leq 100$)
   $n := n + 1$
   end while

   predicate: $2^n < (n + 2)!$

5. loop: **while** ($n \geq 3$ and $n \leq 100$)
   $n := n + 1$
   end while

   predicate: $2n + 1 \leq 2^n$

Exercises 6–9 each contain a while loop annotated with a pre- and a post-condition and also a loop invariant. In each case, use the loop invariant theorem to prove the correctness of the loop with respect to the pre- and post-conditions.

6. *[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $exp = 1$.]*
   while ($i \neq m$)
   1. $exp := exp \cdot x$
   2. $i := i + 1$

   end while

   [Post-condition: $exp = x^m$]
   loop invariant: $I(n)$ is "exp $= x^n$ and $i = n$."

7. *[Pre-condition: largest = A[1] and i = 1]*

while $(i \neq m)$

1. $i := i + 1$
2. **if** $A[i] >$ largest **then** largest $:= A[i]$

end while

[Post-condition: largest = maximum value of $A[1], A[2], \ldots, A[m]$*]*
loop invariant: $I(n)$ is "largest = maximum value of $A[1], A[2], \ldots, A[n+1]$ and $i = n + 1$."

8. *[Pre-condition: sum = A[1] and i = 1]*

while $(i \neq m)$

1. $i := i + 1$
2. sum: = sum + A[i]

end while

[Post-condition: $sum = A[1] + A[2] + \cdots + A[m]$*]*

loop invariant: $I(n)$ is "$i = n + 1$ and $sum = A[1] + A[2] + \cdots + A[n+1]$."

9. *[Pre-condition: a = A and A is a positive integer.]*

while $(a > 0)$

$a := a - 2$

end while

[Post-condition: $a = 0$ *if A is even and* $a = -1$ *if A is odd.]*

loop invariant: $I(n)$ is "Both a and A are even integers or both are odd integers and, in either case, $a \geq -1$."

H* 10. Prove correctness of the **while** loop of Algorithm 4.10.3 (in exercise 27 of Exercise Set 4.10) with respect to the following pre- and post-conditions:

Pre-condition: A and B are positive integers, $a = A$, and $b = B$.

Post-condition: One of a or b is zero and the other is nonzero. Whichever is nonzero equals gcd(A, B).

Use the loop invariant

$I(n)$ "(1) a and b are nonnegative integers with gcd(a, b) = gcd(A, B),
(2) at most one of a and b equals 0,
(3) $0 \leq a + b \leq A + B - n$."

11. The following **while** loop implements a way to multiply two numbers that was developed by the ancient Egyptians.

[Pre-condition: A and B are positive integers, x = A, y = B, and product = 0.]

while $(y \neq 0)$
$r := y \ mod \ 2$
if $r = 0$
then do $x := 2 \cdot x$
$y := y \ div \ 2$
end do
if $r = 1$
then do $product := product + x$
$y := y - 1$
end do
end while

[Post-condition: $product = A \cdot B$*]*

a. Make a trace table to show that the algorithm gives the correct answer for multiplying $A = 13$ times $B = 18$.

b. Prove the correctness of this loop with respect to its pre- and post-conditions by using the loop invariant

$I(n)$: "$xy + product = A \cdot B$."

*** 12.** The following sentence could be added to the loop invariant for the Euclidean algorithm:

There exist integers u, v, s, and t such that $a = uA + vB$ and $b = sA + tB$. 5.5.12

a. Show that this sentence is a loop invariant for

while $(b \neq 0)$
$r := a \ mod \ b$
$a := b$
$b := r$
end while

b. Show that if initially $a = A$ and $b = B$, then sentence (5.5.12) is true before the first iteration of the loop.

c. Explain how the correctness proof for the Euclidean algorithm together with the results of (a) and (b) above allow you to conclude that given any integers A and B with $A > B \geq 0$, there exist integers u and v so that gcd(A, B) = $uA + vB$.

d. By actually calculating u, v, s, and t at each stage of execution of the Euclidean algorithm, find integers u and v so that gcd(330, 156) = $330u + 156v$.

ANSWERS FOR TEST YOURSELF

1. a predicate that describes the initial state of the input variables for the algorithm; a predicate that describes the final state of the output variables for the algorithm **2.** the algorithm variables satisfy the post-condition for the loop **3.** it is true after iteration of the loop **4.** (a) $I(0)$ is true (b) $I(k+1)$ is true after the iteration of the loop (c) the guard G becomes false (d) in the post-condition of the loop

5.6 Defining Sequences Recursively

So, Nat'ralists observe, a Flea/Hath smaller Fleas that on him prey,/And these have smaller Fleas to bite 'em,/And so proceed ad infinitum. —Jonathan Swift, 1733

A sequence can be defined in a variety of different ways. One informal way is to write the first few terms with the expectation that the general pattern will be obvious. We might say, for instance, "consider the sequence 3, 5, 7, ..." Unfortunately, misunderstandings can occur when this approach is used. The next term of the sequence could be 9 if we mean a sequence of odd integers, or it could be 11 if we mean the sequence of odd prime numbers.

The second way to define a sequence is to give an explicit formula for its nth term. For example, a sequence $a_0, a_1, a_2 \ldots$ can be specified by writing

$$a_n = \frac{(-1)^n}{n+1} \quad \text{for every integer } n \geq 0.$$

The advantage of defining a sequence by such an explicit formula is that each term of the sequence is uniquely determined and can be computed in a fixed, finite number of steps by substitution.

The third way to define a sequence is to use recursion, as was done in Examples 5.3.3, 5.4.2, and 5.4.3. This requires giving both an equation, called a *recurrence relation*, that defines each later term in the sequence by reference to earlier terms and also one or more initial values for the sequence. Sometimes it is very difficult or impossible to find an explicit formula for a sequence, but it *is* possible to define the sequence using recursion. Defining sequences recursively is similar to proving theorems by mathematical induction. The recurrence relation is like the inductive step and providing initial values is like proving the basis step. Indeed, the fact that sequences can be defined recursively is equivalent to the fact that mathematical induction works as a method of proof.

Definition

A **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$, where i is an integer with $k - i \geq 0$. If i is a fixed integer, the **initial conditions** for such a recurrence relation specify the values of $a_0, a_1, a_2, \ldots, a_{i-1}$. If i depends on k, the initial conditions specify the values of $a_0, a_1, \ldots, a_m$, where m is an integer with $m \geq 0$.

Example 5.6.1 **Computing Terms of a Recursively Defined Sequence**

Define a sequence $c_0, c_1, c_2, \ldots$ recursively as follows: For every integer $k \geq 2$,

(1) $c_k = c_{k-1} + kc_{k-2} + 1$ recurrence relation

(2) $c_0 = 1$ and $c_1 = 2$ initial conditions

Find c_2, c_3, and c_4.

Solution

$$\begin{aligned} c_2 &= c_1 + 2c_0 + 1 && \text{by substituting } k = 2 \text{ into (1)} \\ &= 2 + 2\cdot 1 + 1 && \text{since } c_1 = 2 \text{ and } c_0 = 1 \text{ by (2)} \end{aligned}$$

$$\begin{aligned} (3)\ \therefore c_2 &= 5 \\ c_3 &= c_2 + 3c_1 + 1 && \text{by substituting } k = 3 \text{ into (1)} \\ &= 5 + 3\cdot 2 + 1 && \text{since } c_2 = 5 \text{ by (3) and } c_1 = 2 \text{ by (2)} \end{aligned}$$

$$\begin{aligned} (4)\ \therefore c_3 &= 12 \\ c_4 &= c_3 + 4c_2 + 1 && \text{by substituting } k = 4 \text{ into (1)} \\ &= 12 + 4\cdot 5 + 1 && \text{since } c_3 = 12 \text{ by (4) and } c_2 = 5 \text{ by (3)} \end{aligned}$$

$$(5)\ \therefore c_4 = 33$$ ■

A given recurrence relation may be expressed in several different ways.

Example 5.6.2 **Writing a Recurrence Relation in More Than One Way**

Note Think of the recurrence relation as $s_{\square} = 3s_{\square - 1} - 1$, where any positive integer expression may be placed in the box $\square$.

Let $s_0, s_1, s_2, \ldots$ be a sequence that satisfies the following recurrence relation:

$$\text{For every integer } k \geq 1, \quad s_k = 3s_{k-1} - 1.$$

Explain why the following statement is true:

$$\text{For every integer } k \geq 0, \quad s_{k+1} = 3s_k - 1.$$

Solution In informal language, the recurrence relation says that any term of the sequence equals 3 times the previous term minus 1. Now for any integer $k \geq 0$, the term previous to s_{k+1} is s_k. Thus for any integer $k \geq 0$, $s_{k+1} = 3s_k - 1$. ■

A sequence defined recursively need not start with a subscript of zero. Also, a given recurrence relation may be satisfied by many different sequences; the actual values of the sequence are determined by the initial conditions.

Example 5.6.3 **Sequences That Satisfy the Same Recurrence Relation**

Let $a_1, a_2, a_3, \ldots$ and $b_1, b_2, b_3, \ldots$ satisfy the recurrence relation that the kth term equals 3 times the $(k-1)$st term for every integer $k \geq 2$:

$$(1)\ a_k = 3a_{k-1} \quad \text{and} \quad b_k = 3b_{k-1}.$$

But suppose that the initial conditions for the sequences are different:

$$(2)\ a_1 = 2 \quad \text{and} \quad b_1 = 1.$$

Find (a) a_2, a_3, a_4 and (b) b_2, b_3, b_4.

Solution

a. $a_2 = 3a_1 = 3\cdot 2 = 6$
$a_3 = 3a_2 = 3\cdot 6 = 18$
$a_4 = 3a_3 = 3\cdot 18 = 54$

b. $b_2 = 3b_1 = 3\cdot 1 = 3$
$b_3 = 3b_2 = 3\cdot 3 = 9$
$b_4 = 3b_3 = 3\cdot 9 = 27$

Thus

$a_1, a_2, a_3, \ldots$ begins 2, 6, 18, 54, . . . and
$b_1, b_2, b_3, \ldots$ begins 1, 3, 9, 27, ... ■

Example 5.6.4 **Showing That a Sequence Given by an Explicit Formula Satisfies a Certain Recurrence Relation**

The sequence of **Catalan numbers**, named after the Belgian mathematician Eugène Catalan (1814–1894), arises in a remarkable variety of different contexts in discrete mathematics. It can be defined as follows: For each integer $n \geq 1$,

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

a. Find C_1, C_2, and C_3.

b. Show that this sequence satisfies the recurrence relation $C_k = \frac{4k-2}{k+1}C_{k-1}$ for every integer $k \geq 2$.

Solution

a. $C_1 = \frac{1}{2}\binom{2}{1} = \frac{1}{2}\cdot 2 = 1, \quad C_2 = \frac{1}{3}\binom{4}{2} = \frac{1}{3}\cdot 6 = 2, \quad C_3 = \frac{1}{4}\binom{6}{3} = \frac{1}{4}\cdot 20 = 5$

Art Collection 3/Alamy Stock Photo

Eugène Catalan (1814–1894)

b. To obtain the kth and $(k-1)$st terms of the sequence, just substitute k and $k-1$ in place of n in the explicit formula for $C_1, C_2, C_3, \ldots$.

$$C_k = \frac{1}{k+1}\binom{2k}{k}$$

$$C_{k-1} = \frac{1}{(k-1)+1}\binom{2(k-1)}{k-1} = \frac{1}{k}\binom{2k-2}{k-1}.$$

Then start with the right-hand side of the recurrence relation and transform it into the left-hand side: For each integer $k \geq 2$,

$$\begin{aligned}
\frac{4k-2}{k+1}C_{k-1} &= \frac{4k-2}{k+1}\left[\frac{1}{k}\binom{2k-2}{k-1}\right] && \text{by substituting}\\
&= \frac{2(2k-1)}{k+1}\cdot\frac{1}{k}\cdot\frac{(2k-2)!}{(k-1)!(2k-2-(k-1))!} && \text{by the formula for } n \text{ choose } r\\
&= \frac{1}{k+1}\cdot(2(2k-1))\cdot\frac{(2k-2)!}{(k(k-1)!)(k-1)!} && \text{by rearranging the factors}\\
&= \frac{1}{k+1}\cdot(2(2k-1))\cdot\frac{1}{k!(k-1)!}\cdot(2k-2)!\cdot\frac{1}{2}\cdot\frac{1}{k}\cdot 2k && \text{because } \tfrac{1}{2}\cdot\tfrac{1}{k}\cdot 2k = 1\\
&= \frac{1}{k+1}\cdot\frac{2}{2}\cdot\frac{1}{k!}\cdot\frac{1}{(k-1)!}\cdot\frac{1}{k}\cdot(2k)\cdot(2k-1)\cdot(2k-2)! && \text{by rearranging the factors}\\
&= \frac{1}{k+1}\cdot\frac{(2k)!}{k!k!} && \text{because } k(k-1)! = k!,\ \tfrac{2}{2} = 1,\\
& && \text{and } 2k\cdot(2k-1)\cdot(2k-2)! = (2k)!\\
&= \frac{1}{k+1}\binom{2k}{k} && \text{by the formula for } n \text{ choose } r\\
&= C_k && \text{by definition of } C_1, C_2, C_3, \ldots.
\end{aligned}$$

■

Examples of Recursively Defined Sequences

Recursion is one of the central ideas of computer science. To solve a problem recursively means to find a way to break it down into smaller subproblems each having the same form as the original problem—and to do this in such a way that when the process is repeated many times, the last of the subproblems are small and easy to solve and the solutions of the subproblems can be woven together to form a solution to the original problem.

Probably the most difficult part of solving problems recursively is to figure out how knowing the solution to smaller subproblems of the same type as the original problem will give you a solution to the problem as a whole. You *suppose* you know the solutions to smaller subproblems and ask yourself how you would best make use of that knowledge to solve the larger problem. The supposition that the smaller subproblems have already been solved has been called the *recursive paradigm* or the *recursive leap of faith*. Once you take this leap, you are right in the middle of the most difficult part of the problem, but generally, the path to a solution from this point, though difficult, is short. The recursive leap of faith is similar to the inductive hypothesis in a proof by mathematical induction.

Example 5.6.5 **The Tower of Hanoi**

Paul Fearn / Alamy Stock Photo

Édouard Lucas (1842–1891)

In 1883 a French mathematician, Édouard Lucas, invented a puzzle that he called the Tower of Hanoi (La Tour D'Hanoï). The puzzle consisted of eight disks of wood with holes in their centers, which were piled in order of decreasing size on one pole in a row of three. A facsimile of the cover of the box is shown in the figure below. Those who played the game were supposed to move all the disks one by one from one pole to another, never placing a larger disk on top of a smaller one. The directions to the puzzle claimed it was based on an old Indian legend:

On the steps of the altar in the temple of Benares, for many, many years Brahmins have been moving a tower of 64 golden disks from one pole to another; one by one, never placing a larger on top of a smaller. When all the disks have been transferred the Tower and the Brahmins will fall, and it will be the end of the world.

The puzzle offered a prize of ten thousand francs (about $45,000 US today) to anyone who could move a tower of 64 disks by hand while following the rules of the game. (See Figure 5.6.1 on the following page.) Assuming that you transferred the disks as efficiently as possible, how many moves would be required to win the prize?

From the paper "La Tour d'Hanoï" by N. Claus (pseudonym for Edouard Lucas), in Science et Nature, vol. 1 (1884) number 8 (January 8), 127–128. Image Courtesy of Paul Stockmeyer.

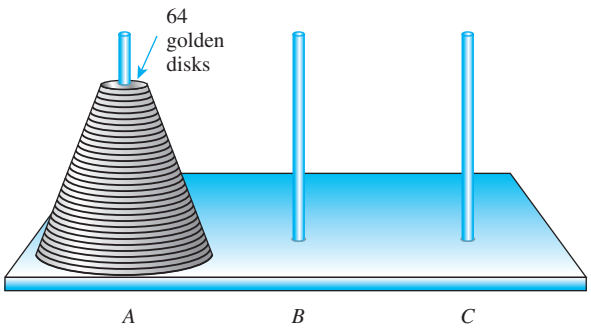


FIGURE 5.6.1

Solution An elegant and efficient way to solve this problem is to think recursively. Suppose that you, somehow or other, have found the most efficient way possible to transfer a tower of $k-1$ disks one by one from one pole to another, obeying the restriction that you never place a larger disk on top of a smaller one. What is the most efficient way to transfer a tower of k disks from one pole to another? The answer is sketched in Figure 5.6.2, where pole A is the initial pole and pole C is the target pole.

Step 1 : Transfer the top $k-1$ disks from pole A to pole B. If $k > 2$, execution of this step will require a number of moves of individual disks among the three poles. But the point of thinking recursively is not to get caught up in imagining the details of how those moves will occur.

Step 2 : Move the bottom disk from pole A to pole C.

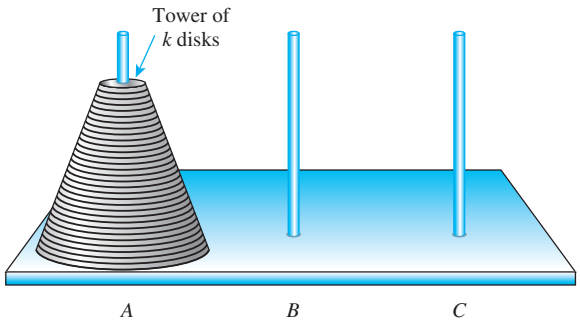
Step 3 : Transfer the top $k-1$ disks from pole B to pole C. (Again, if $k > 2$, execution of this step will require more than one move.)

To see that this sequence of moves is most efficient, observe that to move the bottom disk of a stack of k disks from one pole to another, you must first transfer the top $k-1$ disks to a third pole to get them out of the way. Thus transferring the stack of k disks from pole A to pole C requires at least two transfers of the top $k-1$ disks: one to transfer them off the bottom disk to free the bottom disk so that it can be moved and another to transfer them back on top of the bottom disk after the bottom disk has been moved to pole C. If the bottom disk were not moved directly from pole A to pole C but were moved to pole B first, at least two additional transfers of the top $k-1$ disks would be necessary: one to move them from pole A to pole C so that the bottom disk could be moved from pole A to pole B and another to move them off pole C so that the bottom disk could be moved onto pole C. This would increase the total number of moves and result in a less efficient transfer.

Hence the minimum sequence of moves must include going from the initial position (a) to position (b) to position (c) to position (d). It follows that

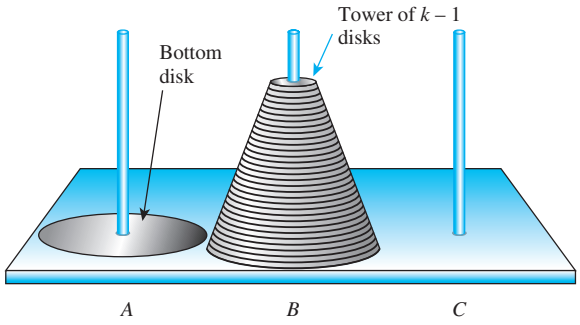
Note Defining the sequence symbolically is a crucial step in solving the problem. The recurrence relation and initial conditions are specified in terms of the sequence.

$$\begin{bmatrix}\text{the minimum number of moves needed to tranfer a tower of } k \text{ disks from pole } A \text{ to pole } C\end{bmatrix} = \begin{bmatrix}\text{the minimum number of moves needed to go from position (a) to position (b)}\end{bmatrix} + \begin{bmatrix}\text{the minimum number of moves needed to go from position (b) to position (c)}\end{bmatrix} + \begin{bmatrix}\text{the minimum number of moves needed to go from position (c) to position (d)}\end{bmatrix}. \quad 5.6.1$$



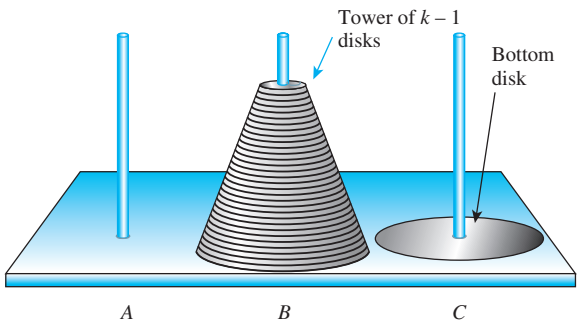
Initial Position

(a)



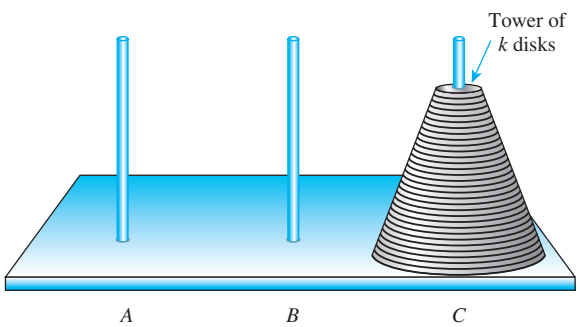
Position after Transferring $k - 1$ Disks from A to B

(b)



Position after Moving the Bottom Disk from A to C

(c)



Position after Transferring $k - 1$ Disks from B to C

(d)

FIGURE 5.6.2 Moves for the Tower of Hanoi

For each integer $n \geq 1$, let

$$m_n = \left[\begin{array}{l}\text{the minimum number of moves needed to transfer} \\ \text{a tower of } n \text{ disks from one pole to another}\end{array}\right].$$

Note that the numbers m_n are independent of the labeling of the poles; it takes the same minimum number of moves to transfer n disks from pole A to pole C as to transfer n disks from pole A to pole B, for example. Also the values of m_n are independent of the number of larger disks that may lie below the top n, provided these remain stationary while the top n are moved. Because the disks on the bottom are all larger than the ones on the top, the top disks can be moved from pole to pole as though the bottom disks were not present.

Going from position (a) to position (b) requires m_{k-1} moves, going from position (b) to position (c) requires just one move, and going from position (c) to position (d) requires m_{k-1} moves. By substitution into equation (5.6.1), therefore,

$$\begin{aligned} m_k &= m_{k-1} + 1 + m_{k-1} \\ &= 2m_{k-1} + 1 \qquad \text{for every integer } k \geq 2. \end{aligned}$$

The initial condition, or base, of this recursion is found by using the definition of the sequence. Because just one move is needed to move one disk from one pole to another,

$$m_1 = \left[\begin{array}{l}\text{the minimum number of moves needed to move} \\ \text{a tower of one disk from one pole to another}\end{array}\right] = 1.$$

Hence the complete recursive specification of the sequence $m_1, m_2, m_3, \ldots$ is as follows: For every integer $k \geq 2$,

$$\begin{aligned} &(1)\ m_k = 2m_{k-1} + 1 && \text{recurrence relation} \\ &(2)\ m_1 = 1 && \text{initial conditions.} \end{aligned}$$

Here is a computation of the next five terms of the sequence:

$$\begin{aligned} &(3)\ m_2 = 2m_1 + 1 = 2 \cdot 1 + 1 = 3 && \text{by (1) and (2)} \\ &(4)\ m_3 = 2m_2 + 1 = 2 \cdot 3 + 1 = 7 && \text{by (1) and (3)} \\ &(5)\ m_4 = 2m_3 + 1 = 2 \cdot 7 + 1 = 15 && \text{by (1) and (4)} \\ &(6)\ m_5 = 2m_4 + 1 = 2 \cdot 15 + 1 = 31 && \text{by (1) and (5)} \\ &(7)\ m_6 = 2m_5 + 1 = 2 \cdot 31 + 1 = 63 && \text{by (1) and (6).} \end{aligned}$$

Going back to the legend, suppose the priests work rapidly and move one disk every second. Then the time from the beginning of creation to the end of the world would be m_{64} seconds. In the next section we derive an explicit formula for m_n. Meanwhile, we can compute m_{64} on a calculator or a computer by continuing the process started above. (Try it!) The approximate result is

$$\begin{aligned} 1.844674 \times 10^{19} \text{ seconds} &\cong 5.84542 \times 10^{11} \text{ years} \\ &\cong 584.5 \text{ billion years,} \end{aligned}$$

which is obtained by the estimate of

$$\begin{array}{ccccccc} 60 & \cdot & 60 & \cdot & 24 & \cdot & (365.25) \\ \uparrow & & \uparrow & & \nwarrow & & \nwarrow \\ \text{seconds per minute} & & \text{minutes per hour} & & \text{hours per day} & & \text{days per year} \end{array} \quad = \quad \begin{array}{c} 31{,}557{,}600 \\ \uparrow \\ \text{seconds per year} \end{array}$$

seconds in a year (figuring 365.25 days in a year to take leap years into account). ■

Example 5.6.6 **The Fibonacci Numbers**

Bettmann/Getty Images

Fibonacci (Leonardo of Pisa) (ca. 1175–1250)

One of the earliest examples of a recursively defined sequence occurs in the writings of Leonardo of Pisa, commonly known as Fibonacci, who was the greatest European mathematician of the Middle Ages and promoted the use of Hindu-Arabic numerals for calculation. In 1202 Fibonacci posed the following problem:

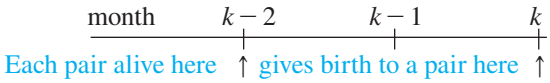
A single pair of rabbits (male and female) is born at the beginning of a year. Assume the following conditions:

1. Rabbit pairs are not fertile during their first month of life but thereafter give birth to one new male/female pair at the end of every month.
2. No rabbits die.

How many rabbits will there be at the end of the year?

Solution One way to solve this problem is to plunge right into the middle of it using recursion. Suppose you know how many rabbit pairs there were at the ends of previous months. How many will there be at the end of the current month?

The crucial observation is that the number of rabbit pairs born at the end of month k is the same as the number of pairs alive at the end of month $k-2$. Why? Because it is exactly the rabbit pairs that were alive at the end of month $k-2$ that were fertile during month k. The rabbits born at the end of month $k-1$ were not.



Now the number of rabbit pairs alive at the end of month k equals the ones alive at the end of month $k-1$ plus the pairs newly born at the end of the month. Thus

Note It is essential to rephrase this observation in terms of a sequence.

$$\begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k\end{bmatrix} = \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k-1\end{bmatrix} + \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs born}\\ \text{at the end}\\ \text{of month } k\end{bmatrix}$$

$$= \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k-1\end{bmatrix} + \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k-2\end{bmatrix}. \qquad 5.6.2$$

For each integer $n \geq 1$, let

$$F_n = \begin{bmatrix}\text{the number of rabbit pairs}\\ \text{alive at the end of month } n\end{bmatrix}$$

and let

$$\begin{aligned} F_0 &= \text{the initial number of rabbit pairs} \\ &= 1. \end{aligned}$$

Then by substitution into equation (5.6.2), for every integer $k \geq 2$,

$$F_k = F_{k-1} + F_{k-2}.$$

Now $F_0 = 1$, as already noted, and $F_1 = 1$ also, because the first pair of rabbits is not fertile until the second month. Hence the complete specification of the Fibonacci sequence is as follows: For every integer $k \geq 2$,

$$\text{(1)}\ F_k = F_{k-1} + F_{k-2} \qquad \text{recurrence relation}$$

$$\text{(2)}\ F_0 = 1, \quad F_1 = 1 \qquad \text{initial conditions.}$$

To answer Fibonacci's question, compute F_2, F_3, and so forth through F_{12}:

$$\text{(3)}\ F_2 = F_1 + F_0 = 1 + 1 = 2 \qquad \text{by (1) and (2)}$$
$$\text{(4)}\ F_3 = F_2 + F_1 = 2 + 1 = 3 \qquad \text{by (1), (2), and (3)}$$
$$\text{(5)}\ F_4 = F_3 + F_2 = 3 + 2 = 5 \qquad \text{by (1), (3), and (4)}$$
$$\text{(6)}\ F_5 = F_4 + F_3 = 5 + 3 = 8 \qquad \text{by (1), (4), and (5)}$$
$$\text{(7)}\ F_6 = F_5 + F_4 = 8 + 5 = 13 \qquad \text{by (1), (5), and (6)}$$
$$\text{(8)}\ F_7 = F_6 + F_5 = 13 + 8 = 21 \qquad \text{by (1), (6), and (7)}$$
$$\text{(9)}\ F_8 = F_7 + F_6 = 21 + 13 = 34 \qquad \text{by (1), (7), and (8)}$$
$$\text{(10)}\ F_9 = F_8 + F_7 = 34 + 21 = 55 \qquad \text{by (1), (8), and (9)}$$
$$\text{(11)}\ F_{10} = F_9 + F_8 = 55 + 34 = 89 \qquad \text{by (1), (9), and (10)}$$
$$\text{(12)}\ F_{11} = F_{10} + F_9 = 89 + 55 = 144 \qquad \text{by (1), (10), and (11)}$$
$$\text{(13)}\ F_{12} = F_{11} + F_{10} = 144 + 89 = 233 \qquad \text{by (1), (11), and (12)}$$

At the end of the twelfth month there are 233 rabbit pairs, or 466 rabbits in all. ■

Example 5.6.7 **Compound Interest**

On your twenty-first birthday you get a letter informing you that on the day you were born an eccentric rich aunt deposited \$100,000 in a bank account earning 4% interest compounded annually and she now intends to turn the account over to you, provided you can figure out how much it is worth. What is the amount currently in the account?

Solution To approach this problem recursively, observe that

$$\begin{bmatrix}\text{the amount in}\\ \text{the account at}\\ \text{the end of any}\\ \text{particular year}\end{bmatrix} = \begin{bmatrix}\text{the amount in}\\ \text{the account at}\\ \text{the end of the}\\ \text{previous year}\end{bmatrix} + \begin{bmatrix}\text{the interest}\\ \text{earned on the}\\ \text{account during}\\ \text{the year}\end{bmatrix}.$$

Now the interest earned during the year equals the interest rate, 4% = 0.04 times the amount in the account at the end of the previous year. Thus

$$\begin{bmatrix}\text{the amount in}\\ \text{the account at}\\ \text{the end of any}\\ \text{particular year}\end{bmatrix} = \begin{bmatrix}\text{the amount in}\\ \text{the account at}\\ \text{the end of the}\\ \text{previous year}\end{bmatrix} + (0.04).\begin{bmatrix}\text{the amount in}\\ \text{the account at}\\ \text{the end of the}\\ \text{previous year}\end{bmatrix}. \qquad 5.6.3$$

For each positive integer n, let

$$A_n = \begin{bmatrix}\text{the amount in the account}\\ \text{at the end of year } n\end{bmatrix}$$

and let

$$A_0 = \begin{bmatrix}\text{the initial amount}\\ \text{in the account}\end{bmatrix} = \$100{,}000.$$

Note Again, a crucial step is to define the sequence symbolically.

Then for any particular year k, substitution into equation (5.6.3) gives

$$\begin{aligned} A_k &= A_{k-1} + (0.04)\cdot A_{k-1} \\ &= (1+0.04)\cdot A_{k-1} = (1.04)\cdot A_{k-1} \qquad \text{by factoring out } A_{k-1}. \end{aligned}$$

Consequently, the values of the sequence $A_0, A_1, A_2, \ldots$ are completely specified as follows: for each integer $k \geq 1$,

$$\begin{aligned} &(1)\ A_k = (1.04)\cdot A_{k-1} \quad \text{recurrence relation} \\ &(2)\ A_0 = \$100{,}000 \quad \text{initial condition.} \end{aligned}$$

The number 1.04 is called the *growth factor* of the sequence.

In the next section we derive an explicit formula for the value of the account in any year n. The value on your twenty-first birthday can also be computed by repeated substitution as follows:

$$\begin{aligned} (3)\ A_1 &= 1.04\cdot A_0 = (1.04)\cdot\$100{,}000 = \$104{,}000 && \text{by (1) and (2)} \\ (4)\ A_2 &= 1.04\cdot A_1 = (1.04)\cdot\$104{,}000 = \$108{,}160 && \text{by (1) and (3)} \\ (5)\ A_3 &= 1.04\cdot A_2 = (1.04)\cdot\$108{,}160 = \$112{,}486.40 && \text{by (1) and (4)} \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ (22)\ A_{20} &= 1.04\cdot A_{19} \cong (1.04)\cdot\$210{,}684.92 \cong \$219{,}112.31 && \text{by (1) and (21)} \\ (23)\ A_{21} &= 1.04\cdot A_{20} \cong (1.04)\cdot\$219{,}112.31 \cong \$227{,}876.81 && \text{by (1) and (22)} \end{aligned}$$

The amount in the account is \$227,876.81 (to the nearest cent). Fill in the dots (to check the arithmetic) and collect your money! ■

Example 5.6.8 **Compound Interest with Compounding Several Times a Year**

When an annual interest rate of i is compounded m times per year, the interest rate paid per period is i/m. (For instance, if $3\% = 0.03$ annual interest is compounded quarterly, then the interest rate paid per quarter is $0.03/4 = 0.0075$.)

For each integer $k \geq 1$, let P_k = the amount on deposit at the end of the kth period, assuming no additional deposits or withdrawals. Then the interest earned during the kth period equals the amount on deposit at the end of the $(k-1)$st period times the interest rate for the period:

$$\text{interest earned during } k\text{th period} = P_{k-1}\left(\frac{i}{m}\right).$$

The amount on deposit at the end of the kth period, P_k, equals the amount at the end of the $(k-1)$st period, P_{k-1}, plus the interest earned during the kth period:

$$P_k = P_{k-1} + P_{k-1}\left(\frac{i}{m}\right) = P_{k-1}\left(1+\frac{i}{m}\right). \qquad 5.6.4$$

Suppose \$10,000 is left on deposit at 3% compounded quarterly.

a. How much will the account be worth at the end of one year, assuming no additional deposits or withdrawals?

b. The **annual percentage yield (APY)** is the percentage increase in the value of the account over a one-year period. What is the APY for this account?

Solution

a. For each integer $n \geq 1$, let P_n = the amount on deposit after n consecutive quarters, assuming no additional deposits or withdrawals, and let P_0 be the initial \$10,000. Then

by equation (5.6.4) with $i = 0.03$ and $m = 4$, a recurrence relation for the sequence $P_0, P_1, P_2, \ldots$ is

(1) $P_k = P_{k-1}(1 + 0.0075) = (1.0075) \cdot P_{k-1}$ for every integer $k \geq 1$.

The amount on deposit at the end of one year (four quarters), P_4, can be found by successive substitution:

(2) $P_0 = \$10{,}000$

(3) $P_1 = 1.0075 \cdot P_0 = (1.0075) \cdot \$10{,}000.00 = \$10{,}075.00$ by (1) and (2)

(4) $P_2 = 1.0075 \cdot P_1 = (1.0075) \cdot \$10{,}075.00 \cong \$10{,}150.56$ by (1) and (3)

(5) $P_3 = 1.0075 \cdot P_2 \cong (1.0075) \cdot \$10{,}150.56 \cong \$10{,}226.69$ by (1) and (4)

(6) $P_4 = 1.0075 \cdot P_3 \cong (1.0075) \cdot \$10{,}226.69 \cong \$10{,}303.39$ by (1) and (5)

Hence after one year there is \$10,303.39 (to the nearest cent) in the account.

b. The percentage increase in the value of the account, or APY, is

$$\frac{10{,}303.39 - 10{,}000}{10{,}000} = 0.03034 = 3.034\%.$$ ■

Recursive Definitions of Sum and Product

Addition and multiplication are called *binary* operations because only two numbers can be added or multiplied at a time. Careful definitions of sums and products of more than two numbers use recursion.

Definition

Given numbers $a_1, a_2, \ldots, a_n$, where n is a positive integer, the **summation from $i = 1$ to n of the a_i**, denoted $\sum_{i=1}^{n} a_i$, is defined as follows:

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n, \quad \text{if } n > 1.$$

The **product from $i = 1$ to n of the a_i**, denoted $\prod_{i=1}^{n} a_i$, is defined by

$$\prod_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n, \quad \text{if } n > 1.$$

The effect of these definitions is to specify an *order* in which sums and products of more than two numbers are computed. For example,

$$\sum_{i=1}^{4} a_i = \left(\sum_{i=1}^{3} a_i\right) + a_4 = \left(\left(\sum_{i=1}^{2} a_i\right) + a_3\right) + a_4 = ((a_1 + a_2) + a_3) + a_4.$$

The recursive definitions are used with mathematical induction to establish various properties of general finite sums and products.

Example 5.6.9 **A Sum of Sums**

Prove that for any positive integer n, if $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are real numbers, then

$$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i.$$

Solution The proof is by mathematical induction. Let the property $P(n)$ be the equation

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i. \qquad \leftarrow P(n)$$

We must show that $P(n)$ is true for every integer $n \geq 1$. We do this by mathematical induction on n.

Show that P(1) is true: To establish $P(1)$, we must show that

$$\sum_{i=1}^{1}(a_i + b_i) = \sum_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i. \qquad \leftarrow P(1)$$

Now

$$\sum_{i=1}^{1}(a_i + b_i) = a_1 + b_1 \qquad \text{by definition of } \Sigma$$

$$= \sum_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i \qquad \text{also by definition of } \Sigma.$$

Hence $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is also true:
Suppose that k is any integer with $k \geq 1$ and that $a_1, a_2, \ldots, a_k, a_{k+1}$ and $b_1, b_2, \ldots, b_k, b_{k+1}$ are real numbers such that

$$\sum_{i=1}^{k}(a_i + b_i) = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i. \qquad \leftarrow P(k) \text{ inductive hypothesis}$$

We must show that

$$\sum_{i=1}^{k+1}(a_i + b_i) = \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i. \qquad \leftarrow P(k+1)$$

[We will show that the left-hand side of this equation equals the right-hand side.]

Now the left-hand side of the equation is

$$\sum_{i=1}^{k+1}(a_i + b_i) = \sum_{i=1}^{k}(a_i + b_i) + (a_{k+1} + b_{k+1}) \qquad \text{by definition of } \Sigma$$

$$= \left(\sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i\right) + (a_{k+1} + b_{k+1}) \qquad \text{by inductive hypothesis}$$

$$= \left(\sum_{i=1}^{k} a_i + a_{k+1}\right) + \left(\sum_{i=1}^{k} b_i + b_{k+1}\right) \qquad \text{by the associative and commutative laws of algebra}$$

$$= \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i \qquad \text{by definition of } \Sigma$$

which equals the right-hand side of the equation. *[This is what was to be shown.]* ■

TEST YOURSELF

1. A recursive definition for a sequence consists of a _____ and _____.

2. A recurrence relation is an equation that defines each later term of a sequence by reference to _____ in the sequence.

3. Initial conditions for a recursive definition of a sequence consist of one or more of the _____ of the sequence.

4. To solve a problem recursively means to divide the problem into smaller subproblems of the same type as the initial problem, to suppose _____, and to figure out how to use the supposition to _____.

5. A crucial step for solving a problem recursively is to define a _____ in terms of which the recurrence relation and initial conditions can be specified.

EXERCISE SET 5.6

Find the first four terms of each of the recursively defined sequences in 1–8.

1. $a_k = 2a_{k-1} + k$, for every integer $k \geq 2$
   $a_1 = 1$

2. $b_k = b_{k-1} + 3_k$, for every integer $k \geq 2$
   $b_1 = 1$

3. $c_k = k(c_{k-1})^2$, for every integer $k \geq 1$
   $c_0 = 1$

4. $d_k = k(d_{k-1})^2$, for every integer $k \geq 1$
   $d_0 = 3$

5. $s_k = s_{k-1} + 2s_{k-2}$, for every integer $k \geq 2$
   $s_0 = 1,\ s_1 = 1$

6. $t_k = t_{k-1} + 2t_{k-2}$, for every integer $k \geq 2$
   $t_0 = -1,\ t_1 = 2$

7. $u_k = ku_{k-1} - u_{k-2}$, for every integer $k \geq 3$
   $u_1 = 1,\ u_2 = 1$

8. $v_k = v_{k-1} + v_{k-2} + 1$, for every integer $k \geq 3$
   $v_1 = 1,\ v_2 = 3$

9. Let $a_0, a_1, a_2, \ldots$ be defined by the formula $a_n = 3n + 1$, for every integer $n \geq 0$. Show that this sequence satisfies the recurrence relation $a_k = a_{k-1} + 3$, for every integer $k \geq 1$.

10. Let $b_0, b_1, b_2, \ldots$ be defined by the formula $b_n = 4^n$, for every integer $n \geq 0$. Show that this sequence satisfies the recurrence relation $b_k = 4b_{k-1}$, for every integer $k \geq 1$.

11. Let $c_0, c_1, c_2, \ldots$ be defined by the formula $c_n = 2^n - 1$ for every integer $n \geq 0$. Show that this sequence satisfies the recurrence relation $c_k = 2c_{k-1} + 1$ for every integer $k \geq 1$.

12. Let $s_0, s_1, s_2, \ldots$ be defined by the formula $s_n = \frac{(-1)^n}{n!}$ for every integer $n \geq 0$. Show that this sequence satisfies the following recurrence relation for every integer $k \geq 1$:

$$s_k = \frac{-s_{k-1}}{k}$$

13. Let $t_0, t_1, t_2, \ldots$ be defined by the formula $t_n = 2 + n$ for every integer $n \geq 0$. Show that this sequence satisfies the following recurrence relation for every integer $k \geq 2$:

$$t_k = 2t_{k-1} - t_{k-2}$$

14. Let $d_0, d_1, d_2, \ldots$ be defined by the formula $d_n = 3^n - 2^n$ for every integer $n \geq 0$. Show that this sequence satisfies the following recurrence relation for every integer $k \geq 2$:

$$d_k = 5d_{k-1} - 6d_{k-2}$$

H 15. For the sequence of Catalan numbers defined in Example 5.6.4, prove that for each integer $n \geq 1$,

$$C_n = \frac{1}{4n+2}\binom{2n+2}{n+1}.$$

16. Use the recurrence relation and values for the Tower of Hanoi sequence $m_1, m_2, m_3, \ldots$ discussed in Example 5.6.5 to compute m_7 and m_8.

17. *Tower of Hanoi with Adjacency Requirement:* Suppose that in addition to the requirement that they never move a larger disk on top of a smaller one, the priests who move the disks of the Tower of Hanoi are also allowed only to move disks one by one from one pole to an *adjacent* pole. Assume poles A and C are at the two ends of the row and pole B is in the middle. Let

$$a_n = \begin{bmatrix}\text{the minimum number of moves}\\ \text{needed to transfer a tower of } n\\ \text{disks from pole } A \text{ to pole } C\end{bmatrix}.$$

   a. Find a_1, a_2, and a_3. **b.** Find a_4.
   c. Find a recurrence relation for $a_1, a_2, a_3, \ldots$. Justify your answer.

18. *Tower of Hanoi with Adjacency Requirement:* Suppose the same situation as in exercise 17. Let

$$b_n = \begin{bmatrix}\text{the minimum number of moves}\\ \text{needed to transfer a tower } \textit{of } n\\ \text{disks from pole } A \text{ to pole } B\end{bmatrix}.$$

a. Find b_1, b_2, and b_3.
b. Find b_4.
c. Show that $b_k = a_{k-1} + 1 + b_{k-1}$ for each integer $k \geq 2$, where $a_1, a_2, a_3, \ldots$ is the sequence defined in exercise 17.
d. Show that $b_k \leq 3b_{k-1} + 1$ for each integer $k \geq 2$.
***H** e.** Show that $b_k = 3b_{k-1} + 1$ for each integer $k \geq 2$.

19. *Four-Pole Tower of Hanoi:* Suppose that the Tower of Hanoi problem has four poles in a row instead of three. Disks can be transferred one by one from one pole to any other pole, but at no time may a larger disk be placed on top of a smaller disk. Let s_n be the minimum number of moves needed to transfer the entire tower of n disks from the left-most to the right-most pole.
a. Find s_1, s_2, and s_3. **b.** Find s_4.
c. Show that $s_k \leq 2s_{k-2} + 3$ for every integer $k \geq 3$.

20. *Tower of Hanoi Poles in a Circle:* Suppose that instead of being lined up in a row, the three poles for the original Tower of Hanoi are placed in a circle. The monks move the disks one by one from one pole to another, but they may only move disks one over in a clockwise direction and they may never move a larger disk on top of a smaller one. Let c_n be the minimum number of moves needed to transfer a pile of n disks from one pole to the next adjacent pole in the clockwise direction.
a. Justify the inequality $c_k \leq 4c_{k-1} + 1$ for each integer $k \geq 2$.
b. The expression $4c_{k-1} + 1$ is not the minimum number of moves needed to transfer a pile of k disks from one pole to another. Explain, for example, why $c_3 \neq 4c_2 + 1$.

21. *Double Tower of Hanoi:* In this variation of the Tower of Hanoi there are three poles in a row and $2n$ disks, two each of n different sizes, where n is any positive integer. Initially one of the poles contains all the disks placed on top of each other in pairs of decreasing size. Disks are transferred one by one from one pole to another, but at no time may a larger disk be placed on top of a smaller disk. However, a disk may be placed on top of one of the same size. Let t_n be the minimum number of moves needed to transfer a tower of $2n$ disks from one pole to another.
a. Find t_1 and t_2. **b.** Find t_3.
c. Find a recurrence relation for $t_1, t_2, t_3, \ldots$.

22. *Fibonacci Variation:* A single pair of rabbits (male and female) is born at the beginning of a year. Assume the following conditions (which are somewhat more realistic than Fibonacci's):
(1) Rabbit pairs are not fertile during their first months of life but thereafter give birth to four new male/female pairs at the end of every month.
(2) No rabbits die.
a. Let r_n = the number of pairs of rabbits alive at the end of month n, for each integer $n \geq 1$, and let $r_0 = 1$. Find a recurrence relation for $r_0, r_1, r_2, \ldots$. Justify your answer.
b. Compute $r_0, r_1, r_2, r_3, r_4, r_5$, and r_6.
c. How many rabbits will there be at the end of the year?

23. *Fibonacci Variation:* A single pair of rabbits (male and female) is born at the beginning of a year. Assume the following conditions:
(1) Rabbit pairs are not fertile during their first *two* months of life, but thereafter give birth to three new male/female pairs at the end of every month.
(2) No rabbits die.
a. Let s_n = the number of pairs of rabbits alive at the end of month n, for each integer $n \geq 1$, and let $s_0 = 1$. Find a recurrence relation for $s_0, s_1, s_2, \ldots$. Justify your answer.
b. Compute s_0, s_1, s_2, s_3, s_4, and s_5.
c. How many rabbits will there be at the end of the year?

In 24–34, $F_0, F_1, F_2, \ldots$ is the Fibonacci sequence.

24. Use the recurrence relation and values for $F_0, F_1, F_2, \ldots$ given in Example 5.6.6 to compute F_{13} and F_{14}.

25. The Fibonacci sequence satisfies the recurrence relation $F_k = F_{k-1} + F_{k-2}$, for every integer $k \geq 2$.
a. Explain why the following is true:
$F_{k+1} = F_k + F_{k-1}$ for each integer $k \geq 1$.
b. Write an equation expressing F_{k+2} in terms of F_{k+1} and F_k.
c. Write an equation expressing F_{k+3} in terms F_{k+2} and F_{k+1}.

26. Prove that $F_k = 3F_{k-3} + 2F_{k-4}$ for every integer $k \geq 4$.

27. Prove that $F_k^2 - F_{k-1}^2 = F_kF_{k+1} - F_{k-1}F_{k+1}$, for every integer $k \geq 1$.

28. Prove that $F_{k+1}^2 - F_k^2 - F_{k-1}^2 = 2F_kF_{k-1}$, for each integer $k \geq 1$.

29. Prove that $F_{k+1}^2 - F_k^2 = F_{k-1}F_{k+2}$, for every integer $k \geq 1$.

30. Use mathematical induction to prove that for each integer $n \geq 0$, $F_{n+2}F_n - F_{n+1}^2 = (-1)^n$.

* **31.** Use strong mathematical induction to prove that $F_n < 2^n$ for every integer $n \geq 1$.

H* **32.** Prove that for each integer $n \geq 0$, $\gcd(F_{n+1}, F_n) = 1$. (The definition of gcd is given in Section 4.10.)

33. It turns out that the Fibonacci sequence satisfies the following explicit formula: For every integer $F_n \geq 0$,

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

Verify that the sequence defined by this formula satisfies the recurrence relation $F_k = F_{k-1} + F_{k-2}$ for every integer $k \geq 2$.

H **34.** (For students who have studied calculus) Find $\lim_{n\to\infty}\left(\frac{F_{n+1}}{F_n}\right)$, assuming that the limit exists.

H* **35.** (For students who have studied calculus) Prove that $\lim_{n\to\infty}\left(\frac{F_{n+1}}{F_n}\right)$ exists.

36. (For students who have studied calculus) Define $x_0, x_1, x_2, \ldots$ as follows:

$$x_k = \sqrt{2 + x_{k-1}} \quad \text{for each integer } k \geq 1$$
$$x_0 = 0.$$

Find $\lim_{n\to\infty} x_n$. (Assume that the limit exists.)

37. *Compound Interest:* Suppose a certain amount of money is deposited in an account paying 4% annual interest compounded quarterly. For each positive integer n, let R_n = the amount on deposit at the end of the nth quarter, assuming no additional deposits or withdrawals, and let R_0 be the initial amount deposited.

- **a.** Find a recurrence relation for $R_0, R_1, R_2, \ldots$. Justify your answer.
- **b.** If $R_0 = \$5{,}000$, find the amount of money on deposit at the end of one year.
- **c.** Find the APY for the account.

38. *Compound Interest:* Suppose a certain amount of money is deposited in an account paying 3% annual interest compounded monthly. For each positive integer n, let S_n = the amount on deposit at the end of the nth month, and let S_0 be the initial amount deposited.

- **a.** Find a recurrence relation for $S_0, S_1, S_2, \ldots$, assuming no additional deposits or withdrawals during the year. Justify your answer.
- **b.** If $S_0 = \$10{,}000$, find the amount of money on deposit at the end of one year.
- **c.** Find the APY for the account.

39. With each step you take when climbing a staircase, you can move up either one stair or two stairs. As a result, you can climb the entire staircase taking one stair at a time, taking two at a time, or taking a combination of one- and two-stair increments. For each integer $n \geq 1$, if the staircase consists of n stairs, let c_n be the number of different ways to climb the staircase. Find a recurrence relation for $c_1, c_2, c_3, \ldots$. Justify your answer.

40. A set of blocks contains blocks of heights 1, 2, and 4 centimeters. Imagine constructing towers by piling blocks of different heights directly on top of one another. (A tower of height 6 cm could be obtained using six 1-cm blocks, three 2-cm blocks one 2-cm block with one 4-cm block on top, one 4-cm block with one 2-cm block on top, and so forth.) Let t_n be the number of ways to construct a tower of height n cm using blocks from the set. (Assume an unlimited supply of blocks of each size.) Find a recurrence relation for $t_1, t_2, t_3, \ldots$. Justify your answer.

41. Assume the truth of the distributive law (Appendix A, F3), and use the recursive definition of summation, together with mathematical induction, to prove the generalized distributive law that for every positive integer n, if $a_1, a_2, \ldots, a_n$ and c are real numbers, then

$$\sum_{i=1}^{n} ca_i = c\left(\sum_{i=1}^{n} a_i\right).$$

42. Assume the truth of the commutative and associative laws (Appendix A, F1 and F2), and use the recursive definition of product, together with mathematical induction, to prove that for every positive integer n, if $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are real numbers, then

$$\prod_{i=1}^{n}(a_ib_i) = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} b_i\right).$$

43. Assume the truth of the commutative and associative laws (Appendix A, F1 and F2), and use the recursive definition of product, together with mathematical induction, to prove that for each positive integer n, if $a_1, a_2, \ldots, a_n$ and c are real numbers, then

$$\prod_{i=1}^{n}(ca_i) = c^n\left(\prod_{i=1}^{n}a_i\right).$$

***H* 44.** The triangle inequality for absolute value states that for all real numbers a and b, $|a+b| \le |a| + |b|$. Use the recursive definition of summation, the triangle inequality, the definition of absolute value, and mathematical induction to prove that for each positive integer n, if $a_1, a_2, \ldots, a_n$ are real numbers, then

$$\left|\sum_{i=1}^{n}a_i\right| \le \sum_{i=1}^{n}|a_i|.$$

45. Prove that any sum of even integers is even.

46. Prove that any sum of an odd number of odd integers is odd.

***H* 47.** Deduce from exercise 46 that for any positive integer n if there is a sum of n odd integers that is even, then n is even.

ANSWERS FOR TEST YOURSELF

1. recurrence relation; initial conditions **2.** earlier terms **3.** values of the first few terms **4.** that the smaller subproblems have already been solved; solve the initial problem **5.** sequence

5.7 Solving Recurrence Relations by Iteration

The keener one's sense of logical deduction, the less often one makes hard and fast inferences. —Bertrand Russell, 1872–1970

Suppose you have a sequence that satisfies a certain recurrence relation and initial conditions. It is often helpful to know an explicit formula for the sequence, especially if you need to compute terms with very large subscripts or if you need to examine general properties of the sequence. Such an explicit formula is called a **solution** to the recurrence relation. In this section, we discuss methods for solving recurrence relations. For example, in the text and exercises of this section, we will show that the Tower of Hanoi sequence of Example 5.6.5 satisfies the formula

$$m_n = 2^n - 1,$$

and that the compound interest sequence of Example 5.6.7 satisfies

$$A_n = (1.04)^n \cdot \$100{,}000.$$

The Method of Iteration

The most basic method for finding an explicit formula for a recursively defined sequence is **iteration**. Iteration works as follows: Given a sequence $a_0, a_1, a_2, \ldots$ defined by a recurrence relation and initial conditions, you start from the initial conditions and calculate successive terms of the sequence until you see a pattern developing. At that point you guess an explicit formula.

Example 5.7.1 **Finding an Explicit Formula**

Let $a_0, a_1, a_2, \ldots$ be the sequence defined recursively as follows: For each integer $k \ge 1$,

(1) $a_k = a_{k-1} + 2$ recurrence relation

(2) $a_0 = 1$ initial condition.

Use iteration to guess an explicit formula for the sequence.

Solution Recall that to say

$$a_k = a_{k-1} + 2 \quad \text{for each integer } k \geq 1$$

means

$$a_{\square} = a_{\square - 1} + 2 \qquad \text{no matter what positive integer is placed into the box } \square.$$

In particular,

$$a_1 = a_0 + 2,$$
$$a_2 = a_1 + 2,$$
$$a_3 = a_2 + 2,$$

and so forth. Now use the initial condition to begin a process of successive substitutions into these equations, not just of numbers (as was done in Section 5.6) but of *numerical expressions*.

The reason for using numerical expressions rather than numbers is that in these problems you are seeking a numerical pattern that underlies a general formula. The secret of success is to leave most of the arithmetic undone. However, you do need to eliminate parentheses as you go from one step to the next. Otherwise, you will soon end up with a bewilderingly large nest of parentheses. Also, it is nearly always helpful to use shorthand notations for regrouping additions, subtractions, and multiplications of numbers that repeat. Thus, for instance, you would write

$$5 \cdot 2 \quad \text{instead of } 2+2+2+2+2$$

and

$$2^5 \quad \text{instead of } 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2.$$

Notice that you don't lose any information about the number patterns when you use these shorthand notations.

Here's how the process works for the given sequence:

$a_0 = 1$ — the initial condition

$a_1 = a_0 + 2 = 1 + 2$ — by substitution

$a_2 = a_1 + 2 = (1 + 2) + 2 = 1 + 2 + 2$ — eliminate parentheses

$a_3 = a_2 + 2 = (1 + 2 + 2) + 2 = 1 + 2 + 2 + 2$ — eliminate parentheses again; write $3 \cdot 2$ instead of $2 + 2 + 2$?

$a_4 = a_3 + 2 = (1 + 2 + 2 + 2) + 2 = 1 + 2 + 2 + 2 + 2$ — eliminate parentheses again; definitely write $4 \cdot 2$ instead of $2 + 2 + 2 + 2$—the length of the string of 2's is getting out of hand.

Tip Do no arithmetic *except*
- replace $n \cdot 1$ and $1 \cdot n$ by n,
- reformat repeated numbers,
- eliminate parentheses.

Since it appears helpful to use the shorthand $k \cdot 2$ in place of $2 + 2 + \cdots + 2$ (k times), we do so, starting again from a_0.

$$
\begin{aligned}
a_0 &= 1 && = 1 + 0\cdot 2 && \text{the initial condition}\\
a_1 &= a_0 + 2 = 1 + 2 && = 1 + 1\cdot 2 && \text{by substitution}\\
a_2 &= a_1 + 2 = (1 + 2) + 2 && = 1 + 2\cdot 2 &&\\
a_3 &= a_2 + 2 = (1 + 2\cdot 2) + 2 && = 1 + 3\cdot 2 &&\\
a_4 &= a_3 + 2 = (1 + 3\cdot 2) + 2 && = 1 + 4\cdot 2 && \text{At this point it certainly seems likely that the general pattern is } 1 + n\cdot 2\text{; check whether the next calculation supports this.}\\
a_5 &= a_4 + 2 = (1 + 4\cdot 2) + 2 && = 1 + 5\cdot 2 && \text{It does! So go ahead and write an answer. It's only a guess, after all.}\\
&\vdots
\end{aligned}
$$

Guess: $a_n = 1 + n\cdot 2 = 1 + 2n$ for every integer n.

The answer obtained for this problem is just a guess. To be sure of the correctness of this guess, you will need to check it by mathematical induction. Later in this section, we will show how to do this. ■

A sequence like the one in Example 5.7.1, in which each term equals the previous term plus a fixed constant, is called an *arithmetic sequence*. In the exercises at the end of this section you are asked to show that the nth term of an arithmetic sequence always equals the initial value of the sequence plus n times the fixed constant.

Definition

A sequence $a_0, a_1, a_2, \ldots$ is called an **arithmetic sequence** if, and only if, there is a constant d such that

$$a_k = a_{k-1} + d \quad \text{for each integer } k \geq 1.$$

It follows that

$$a_n = a_0 + dn \quad \text{for every integer } n \geq 0.$$

Example 5.7.2 **An Arithmetic Sequence**

Under the force of gravity, an object falling in a vacuum falls about 9.8 meters per second (m/sec) faster each second than it fell the second before. Thus, neglecting air resistance, a skydiver's speed upon leaving an airplane is approximately 9.8 m/sec one second after departure, $9.8 + 9.8 = 19.6$ m/sec two seconds after departure, and so forth. If air resistance is neglected, how fast would the skydiver be falling 60 seconds after leaving the airplane?

Solution Let s_n be the skydiver's speed in m/sec n seconds after exiting the airplane, assuming there is no air resistance. Then s_0 is the initial speed, and since the diver would travel 9.8 m/sec faster each second than the second before,

$$s_k = s_{k-1} + 9.8 \text{ m/sec} \quad \text{for every integer } k \geq 1.$$

It follows that $s_0, s_1, s_2, \ldots$ is an arithmetic sequence with a fixed constant of 9.8, and thus

$$s_n = s_0 + (9.8)n \quad \text{for each integer } n \geq 0.$$

Hence sixty seconds after exiting and neglecting air resistance, the skydiver would travel at a speed of

$$s_{60} = 0 + (9.8)(60) = 588 \text{ m/sec}.$$

Now 588 m/sec is over half a kilometer per second or over a third of a mile per second, which is very fast for a human being to travel. Fortunately for the skydiver, taking air resistance into account reduces the speed considerably. ■

In an arithmetic sequence, each term equals the previous term plus a fixed constant. In a geometric sequence, each term equals the previous term *times* a fixed constant. Geometric sequences arise in a large variety of applications, such as compound interest, certain models of population growth, radioactive decay, and the number of operations needed to execute certain computer algorithms.

Example 5.7.3 **The Explicit Formula for a Geometric Sequence**

Let r be a fixed nonzero constant, and suppose a sequence $a_0, a_1, a_2, \ldots$ is defined recursively as follows:

$$a_k = ra_{k-1} \quad \text{for each integer } k \geq 1,$$
$$a_0 = a.$$

Use iteration to guess an explicit formula for this sequence.

Solution

$$a_0 = a$$
$$a_1 = ra_0 = ra$$
$$a_2 = ra_1 = r(ra) = r^2a$$
$$a_3 = ra_2 = r(r^2a) = r^3a$$
$$a_4 = ra_3 = r(r^3a) = r^4a$$
$$\vdots$$

Guess: $a_n = r^n a = ar^n$ for any arbitrary integer $n \geq 0$

In the exercises at the end of this section, you are asked to prove that this formula is correct. ■

Definition

A sequence $a_0, a_1, a_2, \ldots$ is called a **geometric sequence** if, and only if, there is a constant r such that

$$a_k = ra_{k-1} \quad \text{for each integer } k \geq 1.$$

It follows that

$$a_n = a_0 r^n \quad \text{for each integer } n \geq 0.$$

Example 5.7.4 **A Geometric Sequence**

As shown in Example 5.6.7, if a bank pays interest at a rate of 4% per year compounded annually and A_n denotes the amount in the account at the end of year n, then $A_k = (1.04)\,A_{k-1}$, for each integer $k \geq 1$, assuming no deposits or withdrawals during the year. Suppose the initial amount deposited is \$100,000, and assume that no additional deposits or withdrawals are made.

a. How much will the account be worth at the end of 21 years?

b. In how many years will the account be worth \$1,000,000?

Solution

a. $A_0, A_1, A_2, \ldots$ is a geometric sequence with initial value 100,000 and constant multiplier 1.04. Hence,

$$A_n = \$100{,}000 \cdot (1.04)^n \quad \text{for every integer } n \geq 0.$$

After 21 years, the amount in the account will be

$$A_{21} = \$100{,}000 \cdot (1.04)^{21} \cong \$227{,}876.81.$$

This is the same answer as that obtained in Example 5.6.7 but is computed much more easily (at least if a calculator with a powering key, such as $\boxed{\wedge}$ or $\boxed{x^y}$, is used).

b. Let t be the number of years needed for the account to grow to \$1,000,000. Then

$$\$1{,}000{,}000 = \$100{,}000 \cdot (1.04)^t.$$

Dividing both sides by 100,000 gives

$$10 = (1.04)^t,$$

and taking natural logarithms of both sides results in

$$\ln(10) = \ln(1.04)^t.$$

Note Properties of logarithms are reviewed in Section 7.2.

Then

$$\ln(10) \cong t \ln(1.04) \quad \text{because } \log_b(x^a) = a \log_b(x) \text{ (see exercise 35 of Section 7.2)}$$

and so

$$t = \frac{\ln(10)}{\ln(1.04)} \cong 58.7.$$

Hence the account will grow to \$1,000,000 in approximately 58.7 years. ■

An important property of a geometric sequence with constant multiplier greater than 1 is that its terms increase very rapidly in size as the subscripts get larger and larger. For instance, the first ten terms of a geometric sequence with a constant multiplier of 10 are

$$1, \quad 10, \quad 10^2, \quad 10^3, \quad 10^4, \quad 10^5, \quad 10^6, \quad 10^7, \quad 10^8, \quad 10^9.$$

Thus, by its tenth term, the sequence already has the value $10^9 = 1{,}000{,}000{,}000 = 1$ billion. The following box indicates some quantities that are approximately equal to certain powers of 10.

$10^7 \cong$ number of seconds in a year

$10^9 \cong$ number of bytes of memory in a personal computer

$10^{11} \cong$ number of neurons in a human brain

$10^{17} \cong$ age of the universe in seconds (according to one theory)

$10^{31} \cong$ number of seconds to process all possible positions of a checkers game if moves are processed at a rate of 1 per billionth of a second

$10^{81} \cong$ number of atoms in the universe

$10^{111} \cong$ number of seconds to process all possible positions of a chess game if moves are processed at a rate of 1 per billionth of a second

Using Formulas to Simplify Solutions Obtained by Iteration

Explicit formulas obtained by iteration can often be simplified by using formulas such as those developed in Section 5.2. For instance, according to the formula for the sum of a geometric sequence with initial term 1 (Theorem 5.2.2), for each real number r except $r = 1$,

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1} \quad \text{for every integer } n \geq 0.$$

And according to the formula for the sum of the first n integers (Theorem 5.2.1),

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for every integer } n \geq 1.$$

Example 5.7.5 **An Explicit Formula for the Tower of Hanoi Sequence**

Recall that the Tower of Hanoi sequence $m_1, m_2, m_3, \ldots$ of Example 5.6.5 satisfies the recurrence relation

$$m_k = 2m_{k-1} + 1 \quad \text{for each integer } k \geq 2$$

and has the initial condition

$$m_1 = 1.$$

Use iteration to guess an explicit formula for this sequence, and make use of a formula from Section 5.2 to simplify the answer.

Solution By iteration,

$$m_1 = 1$$

$$m_② = 2m_1 + 1 = 2 \cdot 1 + 1 = 2^① + 1,$$

$$m_③ = 2m_2 + 1 = 2(2 + 1) + 1 = 2^② + 2 + 1,$$

$$m_④ = 2m_3 + 1 = 2(2^2 + 2 + 1) + 1 = 2^③ + 2^2 + 2 + 1,$$

$$m_⑤ = 2m_4 + 1 = 2(2^3 + 2^2 + 2 + 1) + 1 = 2^④ + 2^3 + 2^2 + 2 + 1.$$

Caution! Be careful when you use the distributive law. For instance,
$2(2+1)+1 \neq 2^2+1+1$
because
$2(2+1)+1 = 2\cdot 3+1 = 7,$
whereas
$2^2+1+1 = 4+2 = 6.$

These calculations show that each term up to m_5 is a sum of successive powers of 2, starting with $2^0 = 1$ and going up to 2^k, where k is 1 less than the subscript of the term. The pattern would seem to continue to higher terms because each term is obtained from the preceding one by multiplying by 2 and adding 1; multiplying by 2 raises the exponent of each component of the sum by 1, and adding 1 adds back the 1 that was lost when the previous 1 was multiplied by 2. For instance, for $n = 6$,

$$m_6 = 2m_5 + 1 = 2(2^4 + 2^3 + 2^2 + 2 + 1) + 1 = 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1.$$

Thus it seems that, in general,

$$m_n = 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1.$$

By the formula for the sum of a geometric sequence (Theorem 5.2.2),

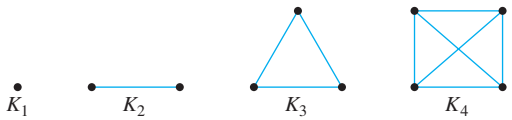
$$2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1 = \frac{2^n - 1}{2-1} = 2^n - 1.$$

Hence the explicit formula seems to be

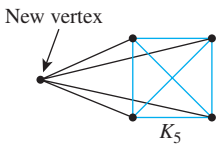
$$m_n = 2^n - 1 \quad \text{for every integer } n \geq 1.$$ ■

Example 5.7.6 **Using Recursion to Compute the Number of Edges of K_n**

In Example 4.9.9 the handshake theorem was used to prove that the number of edges of K_n is $\frac{n(n-1)}{2}$, and in exercise 31 of Section 5.3 you were asked to prove it using mathematical induction. This result can also be obtained using recursion and the formula for the sum of the first n positive integers. Observe that the first few values of K_n can be pictured as follows:



You can obtain K_5 from K_4 by adding one new vertex and drawing four new edges, one each between the new vertex and each vertex of K_4.



Thus

the number of edges of K_5 = the number of edges of K_4 + the 4 new edges.

By the same reasoning, if for each integer $n \geq 1$, s_n is the number of edges of K_n then

$$s_k = s_{k-1} + (k-1) \text{ for each integer } k \geq 2 \qquad \text{recurrence relation}$$
$$s_1 = \text{the number of edges in } K_1 = 0 \qquad \text{initial condition.}$$

Use iteration to find an explicit formula for $s_1, s_2, s_3, \ldots$.

Solution Because

$$s_k = s_{k-1} + (k-1) \quad \text{for each integer } k \geq 2$$

and

$$s_{①} = \underbrace{0}_{1-1},$$

then, in particular,

$$s_{②} = s_1 + 1 = \overbrace{0 + \underbrace{①}_{2-1}}^{\text{1st term}},$$

$$s_{③} = s_2 + 2 = \overbrace{(0+1)}^{\text{1st term}} + 2 = \underbrace{0+1+②}_{3-1},$$

$$s_{④} = s_3 + 3 = \overbrace{(0+1+2)}^{\text{1st term}} + 3 = \underbrace{0+1+2+③}_{4-1},$$

$$s_{⑤} = s_4 + 4 = \overbrace{(0+1+2+3)}^{\text{1st term}} + 4 = 0+1+2+3+\underbrace{④}_{5-1},$$

$$\vdots$$

Guess: $s_{ⓝ} = 0 + 1 + 2 + \cdots + (n-1)$.

By Theorem 5.2.1,

$$0 + 1 + 2 + 3 + \cdots + (n-1) = \frac{(n-1)n}{2} = \frac{n(n-1)}{2}.$$

Hence it appears that

$$s_n = \frac{n(n-1)}{2} \quad \text{for every integer } n \geq 1,$$

which agrees with the results obtained in Sections 4.9 and 5.3. ■

Checking the Correctness of a Formula by Mathematical Induction

As you can see from some of the previous examples, the process of solving a recurrence relation by iteration can involve complicated calculations. It is all too easy to make a mistake and come up with the wrong formula. That is why it is important to confirm your calculations by checking the correctness of your formula. The most common way to do this is to use mathematical induction.

Example 5.7.7 **Using Mathematical Induction to Verify the Correctness of a Solution to a Recurrence Relation**

In Example 5.6.5 we obtained a formula for the Tower of Hanoi sequence. Use mathematical induction to show that this formula is correct.

Solution What does it mean to show the correctness of a formula for a recursively defined sequence? Given a sequence of numbers that satisfies a certain recurrence relation

and initial condition, the job is to show that each term of the sequence satisfies the proposed explicit formula. In this case, you need to prove the following statement:

> If $m_1, m_2, m_3, \ldots$ is the sequence defined by
> $m_k = 2m_{k-1} + 1$ for each integer $k \geq 2$, and
> $m_1 = 1$,
> then $m_n = 2^n - 1$ for every integer $n \geq 1$.

Proof of Correctness: Let $m_1, m_2, m_3, \ldots$ be the sequence defined by specifying that $m_1 = 1$ and $m_k = 2m_{k-1} + 1$ for each integer $k \geq 2$, and let the property $P(n)$ be the equation

$$m_n = 2^n - 1. \qquad \leftarrow P(n)$$

We will use mathematical induction to prove that for every integer $n \geq 1$, $P(n)$ is true.

Show that P(1) is true:
To establish $P(1)$, we must show that

$$m_1 = 2^1 - 1. \qquad \leftarrow P(1)$$

Now the left-hand side of $P(1)$ is

$$m_1 = 1 \qquad \text{by definition of } m_1, m_2, m_3, \ldots,$$

and the right-hand side of $P(1)$ is

$$2^1 - 1 = 2 - 1 = 1.$$

Thus the two sides of $P(1)$ equal the same quantity, and hence $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is also true:
[Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 1$. That is:]
Suppose that k is any integer with $k \geq 1$ such that

$$m_k = 2^k - 1. \qquad \leftarrow P(k) \text{ inductive hypothesis}$$

[We must show that $P(k+1)$ is true. That is:] We must show that

$$m_{k+1} = 2^{k+1} - 1. \qquad \leftarrow P(k+1)$$

But the left-hand side of $P(k+1)$ is

$$\begin{aligned}
m_{k+1} &= 2m_{(k+1)-1} + 1 && \text{by definition of } m_1, m_2, m_3, \ldots \\
&= 2m_k + 1 \\
&= 2(2^k - 1) + 1 && \text{by substitution from the inductive hypothesis} \\
&= 2^{k+1} - 2 + 1 && \text{by the distributive law and the fact that } 2 \cdot 2^k = 2^{k+1} \\
&= 2^{k+1} - 1 && \text{by basic algebra}
\end{aligned}$$

which equals the right-hand side of $P(k+1)$. *[Since the basis and inductive steps have been proved, it follows by mathematical induction that the given formula holds for every integer $n \geq 1$.]* ■

Discovering That an Explicit Formula Is Incorrect

The following example shows how the process of trying to verify a formula by mathematical induction may reveal a mistake.

Example 5.7.8 **Using Verification by Mathematical Induction to Find a Mistake**

Let $c_0, c_1, c_2, \ldots$ be the sequence defined as follows:

$$c_k = 2c_{k-1} + k \quad \text{for each integer } k \geq 1,$$
$$c_0 = 1.$$

Suppose your calculations suggest that $c_0, c_1, c_2, \ldots$ satisfies the following explicit formula:

$$c_n = 2^n + n \quad \text{for every integer } n \geq 0.$$

Is this formula correct?

Solution Start to prove the statement by mathematical induction and see what develops. The proposed formula satisfies the basis step of the inductive proof since on the one hand, $c_0 = 1$ by definition and on the other hand, $2^0 + 0 = 1 + 0 = 1$.

In the inductive step, you suppose that k is any integer with $k \geq 0$ such that

$$c_k = 2^k + k, \qquad \text{This is the inductive hypothesis.}$$

and then you must show that

$$c_{k+1} = 2^{k+1} + (k+1).$$

To do this, you start with c_{k+1}, substitute from the recurrence relation, and use the inductive hypothesis:

$$\begin{aligned} c_{k+1} &= 2c_k + (k+1) && \text{by the recurrence relation} \\ &= 2(2^k + k) + (k+1) && \text{by substitution from the inductive hypothesis} \\ &= 2^{(k+1)} + 3k + 1 && \text{by basic algebra.} \end{aligned}$$

To finish the verification, therefore, you need to show that

$$2^{k+1} + 3k + 1 = 2^{k+1} + (k+1).$$

Now this equation is equivalent to

$$2k = 0 \qquad \text{by subtracting } 2^{k+1} + k + 1 \text{ from both sides}$$

which is equivalent to

$$k = 0 \qquad \text{by dividing both sides by 2.}$$

But this is false since k may be *any* nonnegative integer. For instance, when $k = 1$, then $k + 1 = 2$, and

$$c_2 = 2 \cdot 3 + 2 = 8 \quad \text{whereas} \quad 2^2 + 2 = 4 + 2 = 6.$$

So the formula does not give the correct value for c_2. Hence the sequence $c_0, c_1, c_2, \ldots$ does not satisfy the proposed formula. ■

Once you have found a proposed formula to be false, you should look back at your calculations to see where you made a mistake, correct it, and try again.

TEST YOURSELF

1. To use iteration to find an explicit formula for a recursively defined sequence, start with the _____ and use successive substitution into the _____ to look for a numerical pattern.
2. At every step of the iteration process, it is important to eliminate _____.
3. If a single number, say a, is added to itself k times in one of the steps of the iteration, replace the sum by the expression _____.

4. If a single number, say a, is multiplied by itself k times in one of the steps of the iteration, replace the product by the expression _____.
5. A general arithmetic sequence $a_0, a_1, a_2, \ldots$ with initial value a_0 and fixed constant summand d satisfies the recurrence relation _____ and has the explicit formula _____.
6. A general geometric sequence $a_0, a_1, a_2, \ldots$ with initial value a_0 and fixed constant multiplier r satisfies the recurrence relation _____ and has the explicit formula _____.
7. When an explicit formula for a recursively defined sequence has been obtained by iteration, its correctness can be checked by _____.

EXERCISE SET 5.7

1. The formula
$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$
is true for every integer $n \geq 1$. Use this fact to solve each of the following problems:
   a. If k is an integer and $k \geq 2$, find a formula for the expression $1 + 2 + 3 + \cdots + (k-1)$.
   b. If n is an integer and $n \geq 1$, find a formula for the expression $5 + 2 + 4 + 6 + 8 + \cdots + 2n$.
   c. If n is an integer and $n \geq 1$, find a formula for the expression $3 + 3 \cdot 2 + 3 \cdot 3 + \cdots + 3 \cdot n + n$.

2. The formula
$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$
is true for every real number r except $r = 1$ and for every integer $n \geq 0$. Use this fact to solve each of the following problems:
   a. If i is an integer and $i \geq 1$, find a formula for the expression $1 + 2 + 2^2 + \cdots + 2^{i-1}$.
   b. If n is an integer and $n \geq 1$, find a formula for the expression $3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1$.
   c. If n is an integer and $n \geq 2$, find a formula for the expression $2^n + 2^{n-2} \cdot 3 + 2^{n-3} \cdot 3 + \cdots + 2^2 \cdot 3 + 2 \cdot 3 + 3$.
   d. If n is an integer and $n \geq 1$, find a formula for the expression
$$2^n - 2^{n-1} + 2^{n-2} - 2^{n-3} + \cdots + (-1)^{n-1} \cdot 2 + (-1)^n.$$

In each of 3–15 a sequence is defined recursively. Use iteration to guess an explicit formula for the sequence. Use formulas from Section 5.2 to simplify your answers whenever possible.

3. $a_k = k a_{k-1}$, for each integer $k \geq 1$
   $a_0 = 1$
4. $b_k = \frac{b_{k-1}}{1 + b_{k-1}}$, for each integer $k \geq 1$
   $b_0 = 1$
5. $c_k = 3c_{k-1} + 1$, for each integer $k \geq 2$
   $c_1 = 1$

H 6. $d_k = 2d_{k-1} + 3$, for each integer $k \geq 2$
   $d_1 = 2$

7. $e_k = 4e_{k-1} + 5$, for each integer $k \geq 1$
   $e_0 = 2$
8. $f_k = f_{k-1} + 2^k$, for each integer $k \geq 2$
   $f_1 = 1$

H 9. $g_k = \frac{g_{k-1}}{g_{k-1} + 2}$, for each integer $k \geq 2$
   $g_1 = 1$

10. $h_k = 2^k - h_{k-1}$, for each integer $k \geq 1$
    $h_0 = 1$
11. $p_k = p_{k-1} + 2 \cdot 3^k$ for each integer $k \geq 2$
    $p_1 = 2$
12. $s_k = s_{k-1} + 2k$, for each integer $k \geq 1$
    $s_0 = 3$
13. $t_k = t_{k-1} + 3k + 1$, for each integer $k \geq 1$
    $t_0 = 0$

* 14. $x_k = 3x_{k-1} + k$, for each integer $k \geq 2$
    $x_1 = 1$

15. $y_k = y_{k-1} + k^2$, for each integer $k \geq 2$
    $y_1 = 1$
16. Solve the recurrence relation obtained as the answer to exercise 17(c) of Section 5.6.
17. Solve the recurrence relation obtained as the answer to exercise 21(c) of Section 5.6.
18. Suppose d is a fixed constant and $a_0, a_1, a_2, \ldots$ is a sequence that satisfies the recurrence relation $a_k = a_{k-1} + d$, for each integer $k \geq 1$. Use mathematical induction to prove that $a_n = a_0 + nd$, for every integer $n \geq 0$.
19. A worker is promised a bonus if he can increase his productivity by 2 units a day every day for a

period of 30 days. If on day 0 he produces 170 units, how many units must he produce on day 30 to qualify for the bonus?

20. A runner targets herself to improve her time on a certain course by 3 seconds a day. If on day 0 she runs the course in 3 minutes, how fast must she run it on day 14 to stay on target?

21. Suppose r is a fixed constant and $a_0, a_1, a_2 \ldots$ is a sequence that satisfies the recurrence relation $a_k = ra_{k-1}$, for each integer $k \geq 1$ and $a_0 = a$. Use mathematical induction to prove that $a_n = ar^n$, for every integer $n \geq 0$.

22. As shown in Example 5.6.8, if a bank pays interest at a rate of i compounded m times a year, then the amount of money P_k at the end of k time periods (where one time period $= 1/m$th of a year) satisfies the recurrence relation $P_k = [1 + (i/m)]\, P_{k-1}$ with initial condition $P_0 =$ the initial amount deposited. Find an explicit formula for P_n.

23. Suppose the population of a country increases at a steady rate of 3% per year. If the population is 50 million at a certain time, what will it be 25 years later?

24. A chain letter works as follows: One person sends a copy of the letter to five friends, each of whom sends a copy to five friends, each of whom sends a copy to five friends, and so forth. How many people will have received copies of the letter after the twentieth repetition of this process, assuming no person receives more than one copy?

25. A certain computer algorithm executes twice as many operations when it is run with an input of size k as when it is run with an input of size $k-1$ (where k is an integer that is greater than 1). When the algorithm is run with an input of size 1, it executes seven operations. How many operations does it execute when it is run with an input of size 25?

26. A person saving for retirement makes an initial deposit of \$1,000 to a bank account earning interest at a rate of 3% per year compounded monthly, and each month she adds an additional \$200 to the account.

a. For each nonnegative integer n, let A_n be the amount in the account at the end of n months. Find a recurrence relation relating A_k to A_{k-1}.

H **b.** Use iteration to find an explicit formula for A_n.

c. Use mathematical induction to prove the correctness of the formula you obtained in part (b).

d. How much will the account be worth at the end of 20 years? At the end of 40 years?

H **e.** In how many years will the account be worth \$10,000?

27. A person borrows \$3,000 on a bank credit card at a nominal rate of 18% per year, which is actually charged at a rate of 1.5% per month.

H **a.** What is the annual percentage yield (APY) for the card? (See Example 5.6.8 for a definition of APY.)

b. Assume that the person does not place any additional charges on the card and pays the bank \$150 each month to pay off the loan. Let B_n be the balance owed on the card after n months. Find an explicit formula for B_n.

H **c.** How long will be required to pay off the debt?

d. What is the total amount of money the person will have paid for the loan?

In 28–42 use mathematical induction to verify the correctness of the formula you obtained in the referenced exercise.

28. Exercise 3 **29.** Exercise 4 **30.** Exercise 5

31. Exercise 6 **32.** Exercise 7 **33.** Exercise 8

34. Exercise 9 ***H*** **35.** Exercise 10 **36.** Exercise 11

H **37.** Exercise 12 **38.** Exercise 13 **39.** Exercise 14

40. Exercise 15 **41.** Exercise 16 **42.** Exercise 17

In each of 43–49 a sequence is defined recursively. (a) Use iteration to guess an explicit formula for the sequence. (b) Use strong mathematical induction to verify that the formula of part (a) is correct.

43. $a_k = \dfrac{a_{k-1}}{2a_{k-1} - 1}$, for each integer $k \geq 1$
$a_0 = 2$

44. $b_k = \dfrac{2}{b_{k-1}}$, for each integer $k \geq 2$
$b_1 = 1$

45. $v_k = v_{\lfloor k/2 \rfloor} + v_{\lfloor (k+1)/2 \rfloor} + 2$, for each integer $k \geq 2$
$v_1 = 1$

H **46.** $s_k = 2s_{k-2}$, for each integer $k \geq 2$
$s_0 = 1, s_1 = 2$

47. $t_k = k - t_{k-1}$, for each integer $k \geq 1$
$t_0 = 0$

H **48.** $w_k = w_{k-2} + k$, for each integer $k \geq 3$
$w_1 = 1, w_2 = 2$

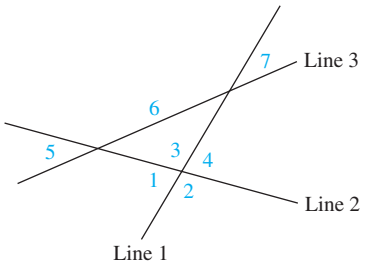
49. $u_k = u_{k-2} \cdot u_{k-1}$, for each integer $k \geq 2$
$u_0 = u_1 = 2$

In 50 and 51 determine whether the given recursively defined sequence satisfies the explicit formula $a_n = (n-1)^2$, for every integer $n \geq 1$.

50. $a_k = 2a_{k-1} + k - 1$, for each integer $k \geq 2$
$a_1 = 0$

51. $a_k = 4a_{k-1} - k + 3$, for each integer $k \geq 2$
$a_1 = 0$

52. A single line divides a plane into two regions. Two lines (by crossing) can divide a plane into four regions; three lines can divide it into seven regions (see the figure). Let P_n be the maximum number of regions into which n lines divide a plane, where n is a positive integer.



a. Derive a recurrence relation for P_k in terms of P_{k-1}, for each integer $k \geq 2$.
b. Use iteration to guess an explicit formula for P_n.

H 53. Compute $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n$ for small values of n (up to about 5 or 6). Conjecture explicit formulas for the entries in this matrix, and prove your conjecture using mathematical induction.

54. In economics the behavior of an economy from one period to another is often modeled by recurrence relations. Let Y_k be the income in period k and C_k be the consumption in period k. In one economic model, income in any period is assumed to be the sum of consumption in that period plus investment and government expenditures (which are assumed to be constant from period to period), and consumption in each period is assumed to be a linear function of the income of the preceding period. That is,

$Y_k = C_k + E$ where E is the sum of investment plus government expenditures

$C_k = c + mY_{k-1}$ where c and m are constants.

Substituting the second equation into the first gives $Y_k = E + c + mY_{k-1}$.

a. Use iteration on the above recurrence relation to obtain

$$Y_n = (E + c)\left(\frac{m^n - 1}{m - 1}\right) + m^n Y_0$$

for every integer $n \geq 1$.

b. (For students who have studied calculus) Show that if $0 < m < 1$, then $\lim_{n \to \infty} Y_n = \frac{E + c}{1 - m}$.

ANSWERS FOR TEST YOURSELF

1. initial conditions; recurrence relation **2.** parentheses **3.** $k \cdot a$ **4.** a^k **5.** $a_k = a_{k-1} + d$; $a_n = a_0 + dn$ **6.** $a_k = ra_{k-1}$; $a_n = a_0 r^n$ **7.** mathematical induction

5.8 Second-Order Linear Homogeneous Recurrence Relations with Constant Coefficients

Genius is 1% inspiration and 99% perspiration. —Thomas Alva Edison, 1932

In Section 5.7 we discussed finding explicit formulas for recursively defined sequences using iteration. This is a basic technique that does not require any special tools beyond the ability to discern patterns. In many cases, however, a pattern is not readily discernible and other methods must be used. A variety of techniques are available for finding explicit formulas for special classes of recursively defined sequences. The method explained in this section is one that works for the Fibonacci and other similarly defined sequences.

Definition

A **second-order linear homogeneous recurrence relation with constant coefficients** is a recurrence relation of the form

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for every integer } k \geq \text{some fixed integer,}$$

where A and B are fixed real numbers with $B \neq 0$.

"Second-order" refers to the fact that the expression for a_k contains the two previous terms a_{k-1} and a_{k-2}, "linear" to the fact that a_{k-1} and a_{k-2} appear in separate terms and to the first power, "homogeneous" to the fact that the total degree of each term is the same (thus there is no constant term), and "constant coefficients" to the fact that A and B are fixed real numbers that do not depend on k.

Example 5.8.1 **Second-Order Linear Homogeneous Recurrence Relations with Constant Coefficients**

State whether each of the following is a second-order linear homogeneous recurrence relation with constant coefficients:

a. $a_k = 3a_{k-1} + 2a_{k-2}$

b. $b_k = b_{k-1} + b_{k-2} + b_{k-3}$

c. $c_k = \frac{1}{2}c_{k-1} - \frac{3}{7}c_{k-2}$

d. $d_k = d_{k-1}^2 + d_{k-1} \cdot d_{k-2}$

e. $e_k = 2e_{k-2}$

f. $f_k = 2f_{k-1} + 1$

g. $g_k = g_{k-1} + g_{k-2}$

h. $h_k = (-1)h_{k-1} + (k-1)h_{k-2}$

Solution

a. Yes; $A = 3$ and $B = 2$

b. No; not second-order

c. Yes; $A = \frac{1}{2}$ and $B = -\frac{3}{7}$

d. No; not linear

e. Yes; $A = 0$ and $B = 2$

f. No; not homogeneous

g. Yes; $A = 1$ and $B = 1$

h. No; nonconstant coefficients ■

The Distinct-Roots Case

Consider a second-order linear homogeneous recurrence relation with constant coefficients:

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for every integer } k \geq 2, \qquad 5.8.1$$

where A and B are fixed real numbers. Relation (5.8.1) is satisfied when each $a_i = 0$, but it has nonzero solutions as well. *Suppose* that for some number t with $t \neq 0$, the sequence

$$1, t, t^2, t^3, \ldots, t^n, \ldots$$

satisfies relation (5.8.1). This means that each term of the sequence equals A times the previous term plus B times the term before that. So for each integer $k \geq 2$,

$$t^k = At^{k-1} + Bt^{k-2}.$$

In particular, when $k = 2$, the equation becomes

$$t^2 = At + B,$$

or, equivalently,

$$t^2 - At - B = 0. \qquad 5.8.2$$

This is a quadratic equation, and the values of t that make it true can be found either by factoring or by using the quadratic formula.

Now work backward. Suppose t is any number that satisfies equation (5.8.2). Does the sequence $1, t, t^2, t^3, \ldots, t^n, \ldots$ satisfy relation (5.8.1)? To answer this question, multiply equation (5.8.2) by t^{k-2} to obtain

$$t^{k-2} \cdot t^2 - t^{k-2} \cdot At - t^{k-2} \cdot B = 0.$$

This is equivalent to

$$t^k - At^{k-1} - Bt^{k-2} = 0,$$

or

$$t^k = At^{k-1} + Bt^{k-2}.$$

Hence the answer is yes: $1, t, t^2, t^3, \ldots, t^n, \ldots$ satisfies relation (5.8.1).

This discussion proves the following lemma.

Lemma 5.8.1

Let A and B be real numbers. A recurrence relation of the form

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for every integer } k \geq 2 \qquad 5.8.1$$

is satisfied by the sequence

$$1, t, t^2, t^3, \ldots, t^n, \ldots,$$

where t is a nonzero real number, if, and only if, t satisfies the equation

$$t^2 - At - B = 0. \qquad 5.8.2$$

Equation (5.8.2) is called the *characteristic equation* of the recurrence relation.

Definition

Given a second-order linear homogeneous recurrence relation with constant coefficients

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for every integer } k \geq 2, \qquad 5.8.1$$

the **characteristic equation of the relation** is

$$t^2 - At - B = 0. \qquad 5.8.2$$

Example 5.8.2 **Using the Characteristic Equation to Find Solutions to a Recurrence Relation**

Consider the recurrence relation that specifies that the kth term of a sequence equals the sum of the $(k-1)$st term plus twice the $(k-2)$nd term. That is,

$$a_k = a_{k-1} + 2a_{k-2} \quad \text{for each integer } k \geq 2. \tag{5.8.3}$$

Find all sequences that satisfy relation (5.8.3) and have the form

$$1, t, t^2, t^3, \ldots, t^n, \ldots,$$

where t is nonzero.

Solution By Lemma 5.8.1, relation (5.8.3) is satisfied by a sequence $1, t, t^2, t^3, \ldots, t^n, \ldots$ if, and only if, t satisfies the characteristic equation

$$t^2 - t - 2 = 0.$$

Since

$$t^2 - t - 2 = (t-2)(t+1),$$

the only possible values of t are 2 and −1. It follows that the sequences

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{and} \quad 1, -1, (-1)^2, (-1)^3, \ldots, (-1)^n, \ldots.$$

are both solutions for relation (5.8.3) and there are no other solutions of this form. Note that these sequences can be rewritten more simply as

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{and} \quad 1, -1, 1, -1, \ldots, (-1)^n, \ldots. \qquad \blacksquare$$

The example above shows how to find two distinct sequences that satisfy a given second-order linear homogeneous recurrence relation with constant coefficients. It turns out that any linear combination of such sequences produces another sequence that also satisfies the relation.

Lemma 5.8.2

If $r_0, r_1, r_2, \ldots$ and $s_0, s_1, s_2, \ldots$ are sequences that satisfy the same second-order linear homogeneous recurrence relation with constant coefficients, and if C and D are *any* numbers, then the sequence $a_0, a_1, a_2, \ldots$ defined by the formula

$$a_n = Cr_n + Ds_n \quad \text{for every integer } n \geq 0$$

also satisfies the same recurrence relation.

Proof: Suppose $r_0, r_1, r_2, \ldots$ and $s_0, s_1, s_2, \ldots$ are sequences that satisfy the same second-order linear homogeneous recurrence relation with constant coefficients. In other words, suppose that for some real numbers A and B,

$$r_k = Ar_{k-1} + Br_{k-2} \quad \text{and} \quad s_k = As_{k-1} + Bs_{k-2} \tag{5.8.4}$$

for every integer $k \geq 2$. Suppose also that C and D are any numbers. Let $a_0, a_1, a_2, \ldots$ be the sequence defined by

$$a_n = Cr_n + Ds_n \quad \text{for every integer } n \geq 0. \tag{5.8.5}$$

[We must show that $a_0, a_1, a_2, \ldots$ satisfies the same recurrence relation as $r_0, r_1, r_2, \ldots$ and $s_0, s_1, s_2, \ldots$. That is, we must show that $a_k = Aa_{k-1} + Ba_{k-2}$, for every integer $k \geq 2$.]

(continued on page 356)

For every integer $k \geq 2$,

$$\begin{aligned} Aa_{k-1} + Ba_{k-2} &= A(Cr_{k-1} + Ds_{k-1}) + B(Cr_{k-2} + Ds_{k-2}) && \text{by substitution from (5.8.5)} \\ &= C(Ar_{k-1} + Br_{k-2}) + D(As_{k-1} + Bs_{k-2}) && \text{by basic algebra} \\ &= Cr_k + Ds_k && \text{by substitution from (5.8.4)} \\ &= a_k && \text{by substitution from (5.8.5).} \end{aligned}$$

Hence $a_0, a_1, a_2, \ldots$ satisfies the same recurrence relation as $r_0, r_1, r_2, \ldots$ and $s_0, s_1, s_2, \ldots$ *[as was to be shown].*

Given a second-order linear homogeneous recurrence relation with constant coefficients, if the characteristic equation has two distinct roots, then Lemmas 5.8.1 and 5.8.2 can be used together to find a particular sequence that satisfies both the recurrence relation and two specific initial conditions.

Example 5.8.3 **Finding the Linear Combination That Satisfies the Initial Conditions**

Find a sequence that satisfies the recurrence relation of Example 5.8.2,

$$a_k = a_{k-1} + 2a_{k-2} \quad \text{for every integer } k \geq 2, \tag{5.8.3}$$

and that also satisfies the initial conditions

$$a_0 = 1 \quad \text{and} \quad a_1 = 8.$$

Solution Consider the following sequences from Example 5.8.2.

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{and} \quad 1, -1, 1, -1, \ldots, (-1)^n, \ldots$$

Both satisfy relation (5.8.3) although neither satisfies the given initial conditions. However, by Lemma 5.8.2, any sequence $a_0, a_1, a_2, \ldots$ that satisfies the explicit formula

$$a_n = C \cdot 2^n + D(-1)^n, \tag{5.8.6}$$

where C and D are numbers, also satisfies relation (5.8.3). You can find C and D so that $a_0, a_1, a_2, \ldots$ satisfies the initial conditions specified in this example by substituting $n = 0$ and $n = 1$ into equation (5.8.6) and solving for C and D:

$$\begin{aligned} a_0 = 1 &= C \cdot 2^0 + D(-1)^0 \\ a_1 = 8 &= C \cdot 2^1 + D(-1)^1. \end{aligned}$$

When you simplify, you obtain the system

$$\begin{aligned} 1 &= C + D \\ 8 &= 2C - D, \end{aligned}$$

which can be solved in various ways. For instance, if you add the two equations, you get

$$9 = 3C,$$

and so

$$C = 3.$$

Then, by substituting into $1 = C + D$, you get

$$D = -2.$$

It follows that the sequence $a_0, a_1, a_2, \ldots$ given by

$$a_n = 3 \cdot 2^n + (-2)(-1)^n = 3 \cdot 2^n - 2(-1)^n,$$

for each integer $n \geq 0$, satisfies both the recurrence relation and the given initial conditions. ■

The techniques of Examples 5.8.2 and 5.8.3 can be used to find an explicit formula for *any* sequence that satisfies a second-order linear homogeneous recurrence relation with constant coefficients for which the characteristic equation has distinct roots, provided that the first two terms of the sequence are known. This is made precise in the next theorem.

Theorem 5.8.3 Distinct-Roots Theorem

Suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2} \tag{5.8.1}$$

for some real numbers A and B with $B \neq 0$ and every integer $k \geq 2$. If the characteristic equation

$$t^2 - At - B = 0 \tag{5.8.2}$$

has two distinct roots r and s, then $a_0, a_1, a_2, \ldots$ is given by the explicit formula

$$a_n = Cr^n + Ds^n,$$

where C and D are the numbers whose values are determined by the values a_0 and a_1.

Note: To say "C and D are determined by the values of a_0 and a_1" means that C and D are the solutions to the system of simultaneous equations

$$a_0 = Cr^0 + Ds^0 \quad \text{and} \quad a_1 = Cr^1 + Ds^1,$$

or, equivalently,

$$a_0 = C + D \quad \text{and} \quad a_1 = Cr + Ds.$$

In exercise 19 at the end of this section you are asked to verify that this system always has a solution when $r \neq s$.

Proof: Suppose that for some real numbers A and B, a sequence $a_0, a_1, a_2, \ldots$ satisfies the recurrence relation $a_k = Aa_{k-1} + Ba_{k-2}$, for every integer $k \geq 2$, and suppose the characteristic equation $t^2 - At - B = 0$ has two distinct roots r and s. We will show that

$$\text{for each integer } n \geq 0, \quad a_n = Cr^n + Ds^n,$$

where C and D are numbers such that

$$a_0 = Cr^0 + Ds^0 \quad \text{and} \quad a_1 = Cr^1 + Ds^1.$$

(continued on page 358)

Let $P(n)$ be the equation

$$a_n = Cr^n + Ds^n. \qquad \leftarrow P(n)$$

We use strong mathematical induction to prove that $P(n)$ is true for each integer $n \geq 0$. In the basis step, we prove that $P(0)$ and $P(1)$ are true. We do this because in the inductive step we need the equation to hold for $n = 0$ and $n = 1$ in order to prove that it holds for $n = 2$.

Show that P(0) and P(1) are true: The truth of $P(0)$ and $P(1)$ is automatic because C and D are exactly those numbers that make the following equations true:

$$a_0 = Cr^0 + Ds^0 \quad \text{and} \quad a_1 = Cr^1 + Ds^1.$$

Show that for every integer k ≥ 1, if P(i) is true for each integer i from 0 through k, then P(k + 1) is also true: Suppose that k is any integer with $k \geq 1$ and for each integer i from 0 through k,

$$a_i = Cr^i + Ds^i \qquad \text{inductive hypothesis.}$$

We must show that

$$a_{k+1} = Cr^{k+1} + Ds^{k+1}. \qquad \leftarrow P(k+1)$$

Now by the inductive hypothesis,

$$a_k = Cr^k + Ds^k \quad \text{and} \quad a_{k-1} = Cr^{k-1} + Ds^{k-1},$$

so

$$\begin{aligned}
a_{k+1} &= Aa_k + Ba_{k-1} && \text{by definition of } a_0, a_1, a_2, \ldots \\
&= A(Cr^k + Ds^k) + B(Cr^{k-1} + Ds^{k-1}) && \text{by inductive hypothesis} \\
&= C(Ar^k + Br^{k-1}) + D(As^k + Bs^{k-1}) && \text{by combining like terms} \\
&= Cr^{k+1} + Ds^{k+1} && \text{by Lemma 5.8.1.}
\end{aligned}$$

This is what was to be shown.

[The reason the last equality follows from Lemma 5.8.1 is that since r and s satisfy the characteristic equation (5.8.2), the sequences $r^0, r^1, r^2, \ldots$ and $s^0, s^1, s^2, \ldots$ satisfy the recurrence relation (5.8.1).]

Remark The t of Lemma 5.8.1 and the C and D of Lemma 5.8.2 and Theorem 5.8.3 are referred to simply as numbers. This is to allow for the possibility of complex as well as real number values. If both roots of the characteristic equation of the recurrence relation are real numbers, then C and D will be real. If the roots are complex but both a_0 and a_1 are real numbers, then C and D will also be real and equal to each other.

The next example shows how to use the distinct-roots theorem to find an explicit formula for the Fibonacci sequence.

Example 5.8.4 **A Formula for the Fibonacci Sequence**

The Fibonacci sequence $F_0, F_1, F_2, \ldots$ satisfies the recurrence relation

$$F_k = F_{k-1} + F_{k-2} \quad \text{for every integer } k \geq 2$$

with initial conditions

$$F_0 = F_1 = 1.$$

Find an explicit formula for this sequence.

Solution The Fibonacci sequence satisfies the first part of the hypothesis of the distinct-roots theorem since the Fibonacci relation is a second-order linear homogeneous recurrence relation with constant coefficients ($A = 1$ and $B = 1$). To check that it satisfies the second part of the hypothesis, examine the characteristic equation

$$t^2 - t - 1 = 0.$$

By the quadratic formula,

$$t = \frac{1 \pm \sqrt{1 - 4(-1)}}{2} = \begin{cases} \dfrac{1+\sqrt{5}}{2} \\ \dfrac{1-\sqrt{5}}{2} \end{cases}$$

and so the roots are distinct. Thus it follows from the distinct-roots theorem that the Fibonacci sequence is given by the explicit formula

$$F_n = C\left(\frac{1+\sqrt{5}}{2}\right)^n + D\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \text{for each integer } n \geq 0, \qquad 5.8.7$$

where C and D are the numbers whose values are determined by the fact that $F_0 = F_1 = 1$. To find C and D, write

$$F_0 = 1 = C\left(\frac{1+\sqrt{5}}{2}\right)^0 + D\left(\frac{1+\sqrt{5}}{2}\right)^0 = C \cdot 1 + D \cdot 1 = C + D$$

and

$$\begin{aligned} F_1 = 1 &= C\left(\frac{1+\sqrt{5}}{2}\right)^1 + D\left(\frac{1-\sqrt{5}}{2}\right)^1 \\ &= C\left(\frac{1+\sqrt{5}}{2}\right) + D\left(\frac{1-\sqrt{5}}{2}\right). \end{aligned}$$

Thus the problem is to find numbers C and D such that

$$C + D = 1$$

and

$$C\left(\frac{1+\sqrt{5}}{2}\right) + D\left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

This may look complicated, but in fact it is just a system of two equations in two unknowns. In exercise 7 at the end of this section, you are asked to solve the system to show that

$$C = \frac{1+\sqrt{5}}{2\sqrt{5}} \quad \text{and} \quad D = \frac{-(1-\sqrt{5})}{2\sqrt{5}}.$$

Substituting these values for C and D into formula (5.8.7) gives

$$F_n = \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{-(1-\sqrt{5})}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

or, simplifying,

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \qquad 5.8.8$$

for each integer $n \geq 0$. Remarkably, even though the formula for F_n involves $\sqrt{5}$, all of the values of the Fibonacci sequence are integers. ■

Note The numbers $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$ are related to the golden ratio of Greek mathematics. See exercise 24 at the end of this section.

The Single-Root Case

Consider again the recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for every integer } k \geq 2, \qquad 5.8.1$$

where A and B are real numbers, but suppose now that the characteristic equation

$$t^2 - At - B = 0 \qquad 5.8.2$$

has a single real root r. By Lemma 5.8.1, one sequence that satisfies the recurrence relation is

$$1, r, r^2, r^3, \ldots, r^n, \ldots.$$

But another sequence that also satisfies the relation is

$$0, r, 2r^2, 3r^3, \ldots, nr^n, \ldots.$$

To see why this is so, observe that since r is the unique root of $t^2 - At - B = 0$, the left-hand side of the equation can be written in the form $(t-r)^2$, and so

$$t^2 - At - B = (t-r)^2 = t^2 - 2rt + r^2. \qquad 5.8.9$$

Equating coefficients in equation (5.8.9) gives

$$A = 2r \quad \text{and} \quad B = -r^2. \qquad 5.8.10$$

Let $s_0, s_1, s_2, \ldots$ be the sequence defined by the formula

$$s_n = nr^n \quad \text{for each integer } n \geq 0.$$

Then

$$\begin{aligned}
As_{k-1} + Bs_{k-2} &= A(k-1)r^{k-1} + B(k-2)r^{k-2} && \text{by definition} \\
&= 2r(k-1)r^{k-1} - r^2(k-2)r^{k-2} && \text{by substitution from 5.8.10} \\
&= 2(k-1)r^k - (k-2)r^k \\
&= (2k-2-k+2)r^k \\
&= kr^k && \text{by basic algebra} \\
&= s_k && \text{by definition.}
\end{aligned}$$

Thus $s_0, s_1, s_2, \ldots$ satisfies the recurrence relation. This argument proves the following lemma.

Lemma 5.8.4

Let A and B be real numbers and suppose the characteristic equation

$$t^2 - At - B = 0$$

has a single root r. Then the sequences $1, r^1, r^2, r^3, \ldots, r^n, \ldots$ and $0, r, 2r^2, 3r^3, \ldots, nr^n, \ldots$ both satisfy the recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for each integer $k \geq 2$.

Lemmas 5.8.2 and 5.8.4 can be used to establish the *single-root theorem*, which tells how to find an explicit formula for any recursively defined sequence satisfying a second-order linear homogeneous recurrence relation with constant coefficients for which the characteristic equation has just one root. Taken together, the distinct-roots and single-root theorems cover all second-order linear homogeneous recurrence relations with constant coefficients. The proof of the single-root theorem is very similar to that of the distinct-roots theorem and is left as an exercise.

Theorem 5.8.5 Single-Root Theorem

Suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for some real numbers A and B with $B \neq 0$ and for every integer $k \geq 2$. If the characteristic equation $t^2 - At - B = 0$ has a single (real) root r, then $a_0, a_1, a_2, \ldots$ is given by the explicit formula

$$a_n = Cr^n + Dnr^n,$$

where C and D are the real numbers whose values are determined by the values of a_0 and any other known value of the sequence.

Example 5.8.5 **Single-Root Case**

Suppose a sequence $b_0, b_1, b_2, \ldots$ satisfies the recurrence relation

$$b_k = 4b_{k-1} - 4b_{k-2} \quad \text{for every integer } k \geq 2, \tag{5.8.11}$$

with initial conditions

$$b_0 = 1 \quad \text{and} \quad b_1 = 3.$$

Find an explicit formula for $b_0, b_1, b_2, \ldots$.

Solution This sequence satisfies part of the hypothesis of the single-root theorem because it satisfies a second-order linear homogeneous recurrence relation with constant coefficients ($A = 4$ and $B = -4$). The single-root condition is also met because the characteristic equation

$$t^2 - 4t + 4 = 0$$

has the unique root $r = 2$ *[since* $t^2 - 4t + 4 = (t-2)^2$*]*.

It follows from the single-root theorem that $b_0, b_1, b_2, \ldots$ is given by the explicit formula

$$b_n = C \cdot 2^n + Dn2^n \quad \text{for each integer } n \geq 0, \tag{5.8.12}$$

where C and D are the real numbers whose values are determined by the fact that $b_0 = 1$ and $b_1 = 3$. To find C and D, write

$$b_0 = 1 = C \cdot 2^0 + D \cdot 0 \cdot 2^0 = C$$

and

$$b_1 = 3 = C \cdot 2^1 + D \cdot 1 \cdot 2^1 = 2C + 2D.$$

Hence the problem is to find numbers C and D such that

$$C = 1$$

and

$$2C + 2D = 3.$$

Substitute $C = 1$ into the second equation to obtain

$$2 + 2D = 3,$$

and so

$$D = \frac{1}{2}.$$

Now substitute $C = 1$ and $D = \frac{1}{2}$ into formula (5.8.12) to conclude that

$$b_n = 2^n + \frac{1}{2}n2^n = 2^n\left(1 + \frac{n}{2}\right) \quad \text{for each integer } n \geq 0. \qquad \blacksquare$$

TEST YOURSELF

1. A second-order linear homogeneous recurrence relation with constant coefficients is a recurrence relation of the form _____ for every integer $k \geq$ _____, where _____.
2. Given a recurrence relation of the form $a_k = Aa_{k-1} + Ba_{k-2}$ for every integer $k \geq 2$, the characteristic equation of the relation is _____.
3. If a sequence $a_1, a_2, a_3, \ldots$ is defined by a second-order linear homogeneous recurrence relation with constant coefficients and the characteristic equation for the relation has two distinct roots r and s (which could be complex numbers), then the sequence is given by an explicit formula of the form _____.
4. If a sequence $a_1, a_2, a_3, \ldots$ is defined by a second-order linear homogeneous recurrence relation with constant coefficients and the characteristic equation for the relation has only a single root r, then the sequence is given by an explicit formula of the form _____.

EXERCISE SET 5.8

1. Which of the following are second-order linear homogeneous recurrence relations with constant coefficients?
   - **a.** $a_k = 2a_{k-1} - 5a_{k-2}$
   - **b.** $b_k = kb_{k-1} + b_{k-2}$
   - **c.** $c_k = 3c_{k-1} \cdot c_{k-2}^2$
   - **d.** $d_k = 3d_{k-1} + d_{k-2}$
   - **e.** $r_k = r_{k-1} - r_{k-2} - 2$
   - **f.** $s_k = 10s_{k-2}$
2. Which of the following are second-order linear homogeneous recurrence relations with constant coefficients?
   - **a.** $a_k = (k-1)a_{k-1} + 2ka_{k-2}$
   - **b.** $b_k = -b_{k-1} + 7b_{k-2}$
   - **c.** $c_k = 3c_{k-1} + 1$
   - **d.** $d_k = 3d_{k-1}^2 + d_{k-2}$
   - **e.** $r_k = r_{k-1} - 6r_{k-3}$
   - **f.** $s_k = s_{k-1} + 10s_{k-2}$

3. Let $a_0, a_1, a_2, \ldots$ be the sequence defined by the explicit formula

$$a_n = C \cdot 2^n + D \quad \text{for every integer } n \geq 0,$$

where C and D are real numbers.

a. Find C and D so that $a_0 = 1$ and $a_1 = 3$. What is a_2 in this case?

b. Find C and D so that $a_0 = 0$ and $a_1 = 2$. What is a_2 in this case?

4. Let $b_0, b_1, b_2, \ldots$ be the sequence defined by the explicit formula

$$b_n = C \cdot 3^n + D(-2)^n \quad \text{for each integer } n \geq 0,$$

where C and D are real numbers.

a. Find C and D so that $b_0 = 0$ and $b_1 = 5$. What is b_2 in this case?

b. Find C and D so that $b_0 = 3$ and $b_1 = 4$. What is b_2 in this case?

5. Let $a_0, a_1, a_2, \ldots$ be the sequence defined by the explicit formula

$$a_n = C \cdot 2^n + D \quad \text{for each integer } n \geq 0,$$

where C and D are real numbers. Show that for any choice of C and D,

$$a_k = 3a_{k-1} - 2a_{k-2} \quad \text{for every integer } k \geq 2.$$

6. Let $b_0, b_1, b_2, \ldots$ be the sequence defined by the explicit formula

$$b_n = C \cdot 3^n + D(-2)^n \quad \text{for every integer } n \geq 0,$$

where C and D are real numbers. Show that for any choice of C and D,

$$b_k = b_{k-1} + 6b_{k-2} \quad \text{for each integer } k \geq 2.$$

7. Solve the system of equations in Example 5.8.4 to obtain

$$C = \frac{1+\sqrt{5}}{2\sqrt{5}} \quad \text{and} \quad D = \frac{-(1-\sqrt{5})}{2\sqrt{5}}.$$

In each of 8–10: (a) suppose a sequence of the form $1, t, t^2, t^3, \ldots, t^n \ldots$ where $t \neq 0$, satisfies the given recurrence relation (but not necessarily the initial conditions), and find all possible values of t: (b) suppose a sequence satisfies the given initial conditions as well as the recurrence relation, and find an explicit formula for the sequence.

8. $a_k = 2a_{k-1} + 3a_{k-2}$, for every integer $k \geq 2$
$a_0 = 1, a_1 = 2$

9. $b_k = 7b_{k-1} - 10b_{k-2}$, for every integer $k \geq 2$
$b_0 = 2, b_1 = 2$

10. $c_k = c_{k-1} + 6c_{k-2}$, for every integer $k \geq 2$
$c_0 = 0, c_1 = 3$

In each of 11–16 suppose a sequence satisfies the given recurrence relation and initial conditions. Find an explicit formula for the sequence.

11. $d_k = 4d_{k-2}$, for each integer $k \geq 2$
$d_0 = 1, d_1 = -1$

12. $e_k = 9e_{k-2}$, for each integer $k \geq 2$
$e_0 = 0, e_1 = 2$

13. $r_k = 2r_{k-1} - r_{k-2}$, for each integer $k \geq 2$
$r_0 = 1, r_1 = 4$

14. $s_k = -4s_{k-1} - 4s_{k-2}$, for every integer $k \geq 2$
$s_0 = 0, s_1 = -1$

15. $t_k = 6t_{k-1} - 9t_{k-2}$, for each integer $k \geq 2$
$t_0 = 1, t_1 = 3$

H 16. $s_k = 2s_{k-1} + 2s_{k-2}$, for every integer $k \geq 2$
$s_0 = 1, s_1 = 3$

17. Find an explicit formula for the sequence of exercise 39 in Section 5.6.

18. Suppose that the sequences $s_0, s_1, s_2, \ldots$ and $t_0, t_1, t_2, \ldots$ both satisfy the same second-order linear homogeneous recurrence relation with constant coefficients:

$$s_k = 5s_{k-1} - 4s_{k-2} \quad \text{for each integer } k \geq 2$$
$$t_k = 5t_{k-1} - 4t_{k-2} \quad \text{for each integer } k \geq 2.$$

Show that the sequence $2s_0 + 3t_0, 2s_1 + 3t_1, 2s_2 + 3t_2, \ldots$ also satisfies the same relation. In other words, show that

$$2s_k + 3t_k = 5(2s_{k-1} + 3t_{k-1}) - 4(2s_{k-2} + 3t_{k-2})$$

for each integer $k \geq 2$. Do *not* use Lemma 5.8.2.

19. Show that if r, s, a_0, and a_1 are numbers with $r \neq s$, then there exist unique numbers C and D so that

$$C + D = a_0$$
$$Cr + Ds = a_1.$$

20. Show that if r is a nonzero real number, k and m are distinct integers, and a_k and a_m are any real numbers, then there exist unique real numbers C and D so that

$$Cr^k + kDr^k = a_k$$
$$Cr^m + mDr^m = a_m.$$

H 21. Prove Theorem 5.8.5 for the case where the values of C and D are determined by a_0 and a_1.

Exercises 22 and 23 are intended for students who are familiar with complex numbers.

22. Find an explicit formula for a sequence $a_0, a_1, a_2, \ldots$ that satisfies

$$a_k = 2a_{k-1} - 2a_{k-2} \quad \text{for every integer } k \geq 2$$

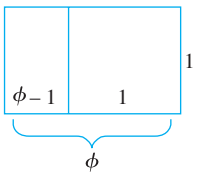
with initial conditions $a_0 = 1$ and $a_1 = 2$.

23. Find an explicit formula for a sequence $b_0, b_1, b_2, \ldots$ that satisfies

$$b_k = 2b_{k-1} - 5b_{k-2} \quad \text{for each integer } k \geq 2$$

with initial conditions $b_0 = 1$ and $b_1 = 1$.

24. The numbers $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$ that appear in the explicit formula for the Fibonacci sequence are related to a quantity called the *golden ratio* in Greek mathematics. Consider a rectangle of length ϕ units and height 1, where $\phi > 1$.



Divide the rectangle into a rectangle and a square as shown in the preceding diagram. The square is 1 unit on each side, and the rectangle has sides of lengths 1 and $\phi - 1$. The ancient Greeks considered the outer rectangle to be perfectly proportioned (saying that the lengths of its sides are in a *golden ratio* to each other) if the ratio of the length to the width of the outer rectangle equals the ratio of the length to the width of the inner rectangle. That is, if the number ϕ satisfies the equation

$$\frac{\phi}{1} = \frac{1}{\phi - 1}.$$

a. Show that if ϕ satisfies the equation above, then it also satisfies the quadratic equation: $t^2 - t - 1 = 0$.
b. Find the two solutions of $t^2 - t - 1 = 0$ and call them ϕ_1 and ϕ_2.
c. Express the explicit formula for the Fibonacci sequence in terms of ϕ_1 and ϕ_2.

ANSWERS FOR TEST YOURSELF

1. $a_k = Aa_{k-1} + Ba_{k-2}$; 2; A and B are fixed real numbers with $B \neq 0$ **2.** $t^2 - At - B = 0$ **3.** $a_n = Cr^n + Ds^n$, where C and D are real or complex numbers **4.** $a_n = Cr^n + Dnr^n$, where C and D are real numbers

5.9 General Recursive Definitions and Structural Induction

GENIE: Oh, aren't you acquainted with recursive acronyms? I thought everybody knew about them. You see, "GOD" stands for "GOD Over Djinn"—which can be expanded as "GOD Over Djinn, Over Djinn"—and that can, in turn, be expanded to "GOD Over Djinn, Over Djinn, Over Djinn"—which can, in its turn, be further expanded.... You can go as far as you like.
ACHILLES: But I'll never finish!
GENIE: Of course not. You can never totally expand GOD.
—Douglas Hofstadter, *Gödel, Escher, Bach*, 1979

Sequences of numbers are not the only objects that can be defined recursively. In this section we discuss recursive definitions for sets and functions. We also introduce *structural induction*, which is a version of mathematical induction that is used to prove properties of recursively defined sets.

Recursively Defined Sets

To define a set of objects recursively, you identify a few core objects as belonging to the set and give rules showing how to build new set elements from old. More formally, a recursive definition for a set consists of the following three components:

I. **Base:** A statement that certain objects belong to the set.

II. **Recursion:** A collection of rules indicating how to form new set objects from those already known to be in the set.

III. **Restriction:** A statement that no objects belong to the set other than those coming from the base and the recursion.

Example 5.9.1 **Recursive Definition of Boolean Expressions**

Note An example of a "legal" expression is $p \wedge (q \vee \sim r)$, and an example of an "illegal" one is $\wedge \sim pqr \vee$.

The set of Boolean expressions was introduced in Section 2.4 as "legal" expressions involving letters from the English alphabet such as p, q, and r, and the symbols $\wedge$, $\vee$, $\sim$, and ( ). To make precise which expressions are legal, the set of Boolean expressions over a general alphabet is defined recursively.

I. Base: Each symbol of the alphabet is a Boolean expression.

II. Recursion: If P and Q are Boolean expressions, then the following are also Boolean expressions:

$$\text{II(a) } P \wedge Q \quad \text{II(b) } P \vee Q \quad \text{II(c) } \sim P \quad \text{II(d) } (P)$$

III. Restriction: There are no Boolean expressions over the alphabet other than those obtained from the base and the recursion.

Derive the fact that the following is a Boolean expression over the English alphabet $\{a, b, c, \ldots, x, y, z\}$:

$$\sim(p \wedge q) \vee (\sim r \wedge p).$$

Solution (1) By I, p, q, and r are Boolean expressions.

(2) By (1), II(a), and II(c), $p \wedge q$ and $\sim r$ are Boolean expressions.

(3) By (2), II(d), and II(a), $(p \wedge q)$ and $\sim r \wedge p$ are Boolean expressions.

(4) By (3), II(c), and II(d), $\sim(p \wedge q)$ and $(\sim r \wedge p)$ are Boolean expressions.

(5) By (4) and II(b), $\sim(p \wedge q) \vee (\sim r \wedge p)$ is a Boolean expression. ■

Example 5.9.2 **Recursive Definition of Parenthesis Structures**

Certain configurations of parentheses in algebraic expressions are "legal" *[such as* (())() *and* ()()()*]*, whereas others are not *[such as*)( )) *and* ()))(((*]*. Here is a recursive definition to generate the set C of legal parenthesis structures.

I. Base: ( ) is in C.

II. Recursion:
II(a) If E is in C, so is (E).
II(b) If E and F are in C, so is EF.

III. Restriction: No parenthesis structures are in P other than those obtained from the base and the recursion.

Show that (( ))( ) is a parenthesis structure in C.

Solution (1) By I, ( ) is in C.

(2) By (1) and II(a), (( )) is in C.

(3) By (2), (1), and II(b), (( ))( ) is in C.

Recursion is used to give a formal definition for the set of all strings over a finite set. ■

Recursive Definition for the Set of All Strings over a Finite Set

Let A be any finite set. Call the elements of A **characters**, and define the **set S of all strings over A** as follows:

I. Base: λ is a string in S, where λ denotes the **null string**, the "string" with no characters.

II. Recursion: New strings are formed according to the following rules:

II(a) If u is any string in S and if c is any character in A, then

$$uc \text{ is a string in } S,$$

where uc is called the **concatenation of u and c**, and is obtained by appending c on the right of u.

II(b) If u is any string in S, then both the concatenation of λ and u, denoted λu, and the concatenation of u and λ, denoted $u\lambda$, are defined to equal u. Symbolically:

$$\lambda u = u\lambda = u.$$

II(c) If u and v are any strings in S, and if c is any character in A, then the concatenation of u and vc is defined to equal the concatenation of uv and c. Symbolically:

$$u(vc) = (uv)c.$$

III. Restriction: Nothing is a string in S other than objects obtained from the base and the recursion.

The base for the recursive definition of strings indicates only that one character, namely λ, is a string. The next theorem states that each individual character in the underlying set is a string.

Theorem 5.9.1 Characters Are Strings

If A is a finite set and S is the set of all strings over A, then every character in A is a string in S.

Proof:

(1) Suppose c is any character in A.

(2) By part I of the definition of string, λ is a string in S.

(3) By part II(a) of the definition of string, λc is a string in S.

(4) By part I of the definition of string, $\lambda c = c$.

(5) Thus c is a string in S.

Example 5.9.3 **Proving a Property of Strings**

Suppose A is a finite set, S is the set of all strings over A, and a and b are in A. Because of the way the definition of string is stated, it cannot be deduced immediately that $b(aa)$ is a string in S. To prove that this is true, first show that ba and $(ba)a$ are strings in S and use the fact that $b(aa) = (ba)a$.

Solution (1) By Theorem 5.9.1, a and b are strings in S because both a and b are in A.

(2) By (1) and II(a), ba is a string in S because b is in S and $a \in A$.

(3) By (2) and II(a), $(ba)a$ is a string in S because $ba \in S$ and $a \in A$.

(4) By II(c), $b(aa) = (ba)a$ because b and a are strings in S and $a \in A$.

(5) By (3) and (4), $b(aa)$ is a string in S because it equals $(ba)a$, which is a string in S. ■

Example 5.9.4 **Sets of Strings with Certain Properties**

In *Gödel, Escher, Bach*, Douglas Hofstadter introduces the following recursively defined set of strings of M's, I's, and U's, which he calls the MIU-system.*

I. Base: MI is in the MIU-system.

II. Recursion:

II(a) If $x\,I$ is in the MIU-system, where x is a string, then $x\,IU$ is in the MIU-system. (In other words, you can add a U to any string that ends in I. For example, since MI is in the system, so is MIU.)

II(b) If Mx is in the MIU-system, where x is a string, then Mxx is in the MIU-system. (In other words, you can repeat all the characters in a string that follow an initial M. For example, if MUI is in the system, so is $MUIUI$.)

II(c) If $xIIIy$ is in the MIU-system, where x and y are strings (possibly null), then $x\,U\,y$ is also in the MIU-system. (In other words, you can replace III by U. For example, if $MIIII$ is in the system, so are MIU and MUI.)

II(d) If $x\,UU\,y$ is in the MIU-system, where x and y are strings (possibly null), then xUy is also in the MIU-system. (In other words, you can replace UU by U. For example, if $MIIUU$ is in the system, so is $MIIU$.)

III. Restriction: No strings other than those derived from I and II are in the MIU-system.

Derive the fact that $MUIU$ is in the MIU-system.

Solution (1) By I, MI is in the MIU-system.

(2) By (1) and II(b), MII is in the MIU-system.

(3) By (2) and II(b), $MIIII$ is in the MIU-system.

(4) By (3) and II(c), MUI is in the MIU-system.

(5) By (4) and II(a), $MUIU$ is in the MIU-system. ■

Proving Properties about Recursively Defined Sets

When a set has been defined recursively, a version of mathematical induction, called **structural induction**, can be used to prove that every object in the set satisfies a given property.

*Douglas Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid* (New York: Basic Books, 1979), pp. 33–35.

Structural Induction for a Recursively Defined Set

Let S be a set that has been defined recursively, and let $P(x)$ be a property that objects in S may or may not satisfy. To prove that every object in S satisfies $P(x)$, perform the following two steps:

Step 1 (basis step): Show that $P(a)$ is true for each object a in the base for S.
Step 2 (inductive step): Show that for each x in S, if $P(x)$ is true and if y is obtained from x by applying a rule from the recursion, then $P(y)$ is true. To perform this step,

> **suppose** that x is an arbitrarily chosen element of S for which $P(x)$ is true.
>
> *[This supposition is the **inductive hypothesis**.]*

Then

> **show** that if y is obtained from x by applying a rule from the recursion for S, then $P(y)$ is true.

Conclusion: Because no objects other than those obtained from the base and recursion are contained in S, steps 1 and 2 prove that $P(x)$ is true for every object x in S.

Example 5.9.5 **A Property of the Set of Integers**

Let S be the set of all integers defined recursively as follows:

I. Base: 4 is in S.

II. Recursion: Given any integer n in S, $n + 3$ is in S.

III. Restriction: No integers are in S other than those derived from the base and the recursion.

Use structural induction to prove that for every integer n in S, $n \bmod 3 = 1$.

Solution

Proof (by structural induction): Given any integer n in S, let property $P(n)$ be the sentence "$n \bmod 3 = 1$."

Show that P(n) is true for each integer n in the base for S:
The only object in the base for S is 4, and $P(4)$ is true because $4 \bmod 3 = 1$ since $4 = 3 \cdot 1 + 1$.

Show that for each integer n in S, if P(n) is true and if m is obtained from n by applying a rule from the recursion for S, then P(m) is true:

Suppose n is any integer in S such that $P(n)$ is true. Then $n \bmod 3 = 1$. *[This is the inductive hypothesis.]* The recursion for S consists only of one rule, and when the rule is applied to n, the result is $n + 3$. To complete the inductive step, we must show that $P(n + 3)$ is true. By inductive hypothesis,

$$n = 3k + 1 \quad \text{for some integer } k.$$

It follows that

$$\begin{aligned} (n+3) \bmod 3 &= [(3k+1)+3] \bmod 3 && \text{by substitution} \\ &= (3k+4) \bmod 3 && \text{by basic algebra} \\ &= [3(k+1)+1] \bmod 3 && \text{because } k+1 \text{ is an integer,} \\ &= 1 \end{aligned}$$

which means that $P(n + 3)$ is true *[as was to be shown]*.

Conclusion:
Because there are no integers in S other than those obtained from the base and the recursion for S, every integer n in S satisfies the equation $n \bmod 3 = 1$. ■

Example 5.9.6 **A Property of the Set of Parentheses**

Consider the set C of all legal configurations of parentheses defined in Example 5.9.2. Use structural induction to prove that every configuration in C contains an equal number of left and right parentheses.

Solution

Proof (by structural induction): Given any parenthesis structure x in C, let property $P(x)$ be the sentence "x has an equal number of left and right parentheses."

Show that P(a) is true for each parenthesis structure in the base for C:
The only object a in the base for C is ( ), which has one left parenthesis and one right parenthesis. Since these numbers are equal, $P(a)$ is true.

Show that for each parenthesis structure x in C, if P(x) is true and if y is obtained from x by applying a rule from the recursion for C, then P(y) is true:
The recursion for C in Example 5.9.2 consists of two rules: II(a) and II(b).

Suppose E and F are any parenthesis structures in C such that $P(E)$ and $P(F)$ are true. In other words, E has an equal number, say n, of left and right parentheses, and F has an equal number, say m, of left and right parentheses. *[This is the inductive hypothesis.]*

When rule II(a) is applied to E, the result is (E), which has $n + 1$ left parentheses and $n + 1$ right parentheses. Since these numbers are equal, $P((E))$ is true. When rule II(b) is applied to E and F, the result is EF, which has an equal number, namely $m + n$, of left and right parentheses. So $P(EF)$ is true.

Thus when the recursion rules for C are applied to parenthesis structures that have an equal number of left and right parentheses, the results also have an equal number of left and right parentheses, which completes the inductive step.

Conclusion:
Because there are no parenthesis structures in C other than those obtained from the base and the recursion for C, every parenthesis structure in C has an equal number of left and right parentheses. ■

Consider the recursive definition for the set of all strings S over a finite set A given on page 366. A recursive definition can also be given for the length of a string.

Definition Length of a String

Given the set of all strings S over a finite set A, the **length L of a string in S** in defined as follows:

1. $L(\lambda) = 0$.
2. For every string u in S and for every character a in A, the length of ua is one more than the length of u. Symbolically:

$$L(ua) = L(u) + 1 \quad \text{where} \quad u \in S \text{ and } a \in A.$$

The following theorem states that the length of a concatenation of two strings is the sum of the lengths of the strings.

Theorem 5.9.2 Additive Property of String Length

If S is the set of all strings over a finite set A, then for all strings u and v in S, $L(uv) = L(u) + L(v)$.

Proof (by structural induction): Let S be the set of all strings over a finite set A. Given any string v in S, let the property $P(v)$ be the sentence

$$\text{For every string } u \text{ in } S, \quad L(uv) = L(u) + L(v).$$

We will show that $P(v)$ is true for every string v in S.

Show that P(a) is true for each string a in the base for S:

The only string in the base for S is λ, and if u is any string in S, then

$$\begin{aligned} L(u\lambda) &= L(u) && \text{by part II(b) in the definition of string} \\ &= L(u) + 0 && \text{by definition of } L. \\ &= L(u) + L(\lambda) \end{aligned}$$

This shows that $P(\lambda)$ is true.

Show that for each string x in S, if P(x) is true and if y is obtained from x by applying a rule from the recursion for S, then P(y) is true:

The recursion for S consists of three rules denoted II(a), II(b), and II(c), but rule II(a) is the only one that generates new strings in S. Suppose v is any string in S such that $P(v)$ is true. In other words, suppose that $L(uv) = L(u) + L(v)$. *[This is the inductive hypothesis.]*

When rule II(a) is applied to v, the result is vc, where c is a character in A. So, to complete the inductive step, we must show that $P(vc)$ is true. Now

$$\begin{aligned} L(u(vc)) &= L((uv)c) && \text{by part II(c) of the definition of string} \\ &= L(uv) + 1 && \text{by definition of length of a string} \\ &= (L(u) + L(v)) + 1 && \text{because } u \text{ is assumed to satisfy property } P \\ &= L(u) + (L(v) + 1) && \text{by the associative law for addition} \\ &= L(u) + L(vc) && \text{by definition of length of a string.} \end{aligned}$$

Hence $P(vc)$ is true *[as was to be shown].*

Conclusion:

Because there are no strings in S other than those obtained through the base and the recursion for S, we conclude that every string in S satisfies the additive property for string length.

The definition of string only defined concatenation between a string and an element of the underlying set. The next theorem extends the operation to pairs of strings.

Theorem 5.9.3 The Concatenation of Any Two Strings Is a String

If S is the set of all strings over a finite set A and u and v are any strings in S, then uv is a string in S.

Proof (by structural induction): Let S be the set of all strings over a finite set A. Given any string v in S, let the property $P(v)$ be the sentence

For every string u in S, uv is a string in S.

We will show that $P(v)$ is true for every string v in S.

Show that P(a) is true for each string a in the base for S:
The only string in the base for S is λ, and if u is any string in S, then, by rule II(b) in the definition of string, $u\lambda = u$. Hence the concatenation of u and λ is a string in S, and so $P(\lambda)$ is true.

Show that for each string x in S, if P(x) is true and if y is obtained from x by applying a rule from the recursion for S, then P(y) is true:
The recursive definition for S consists of three rules denoted II(a), II(b), and II(c), but rule II(a) is the only one that generates new strings in S. Suppose v is any string in S such that $P(v)$ is true. In other words, suppose that for every string u in S, uv is a string in S. *[This is the inductive hypothesis.]*

When rule II(a) is applied to v, the result is vc, where c is a character in A. To complete the inductive step, we must show that $P(vc)$ is true. To do so, we will show that $u(vc)$ is a string in S.

Now because uv is a string in S, it follows from rule II(a) that $(uv)c$ is also a string in S. In addition, by rule II(c),

$$(uv)c = u(vc).$$

Therefore, $u(vc)$ is a string in S, which means that $P(vc)$ is true *[as was to be shown].*

Conclusion:
Because there are no strings in S other than those obtained from the base and the recursion for S, we conclude that the concatenation of any two strings in S is a string in S.

Part II(c) of the definition of string states that a concatenation of three strings of a certain type is associative—but only when the rightmost string is an element in the underlying set. The next theorem generalizes the associativity of concatenation to any three strings.

Theorem 5.9.4 Concatenation of Strings Is Associative

If S is the set of all strings over a finite set A and u, v, and w are any strings in S, then $u(vw) = (uv)w$.

Idea of a proof by structural induction: Let S be the set of all strings over a finite set A. Given any string w in S, let the property $P(w)$ be the sentence

For all strings u and v in S, $u(vw) = (uv)w$.

(continued on page 372)

The proof must show (1) that $P(\lambda)$ is true, and (2) that if w is any string in S such that $P(w)$ is true and if y is obtained from w by applying a rule from the recursion for S, then $P(y)$ is true. Now when rule II(a) is applied to w the result is wc for some character c in A. A crucial step is to show that $u((vw)c) = (u(vw))c$. This follows from the definition of string because u and vw are in S and c is in A.

Exercise 21 at the end of this section asks you to write a complete proof.

Recursive Functions

A function is said to be **defined recursively** or to be a **recursive function** if its rule of definition refers to itself. Because of this self-reference, it is sometimes difficult to tell whether a given recursive function is well defined. Recursive functions are of great importance in the theory of computation in computer science.

Example 5.9.7 **McCarthy's 91 Function**

AP Photo

John McCarthy (1927–2011)

The following function $M : \mathbf{Z}^+ \to \mathbf{Z}$ was defined by John McCarthy, a pioneer in the theory of computation and in the study of artificial intelligence:

$$M(n) = \begin{cases} n - 10 & \text{if } n > 100 \\ M(M(n + 11)) & \text{if } n \leq 100 \end{cases}$$

for all positive integers n. Find $M(99)$.

Solution By repeated use of the definition of M,

$$\begin{aligned} M(99) &= M(M(110)) && \text{since } 99 \leq 100 \\ &= M(100) && \text{since } 110 > 100 \\ &= M(M(111)) && \text{since } 100 \leq 100 \\ &= M(101) && \text{since } 111 > 100 \\ &= 91 && \text{since } 101 > 100. \end{aligned}$$

The remarkable thing about this function is that it takes the value 91 for all positive integers less than or equal to 101. (You are asked to show this in exercise 24 at the end of this section.) For $n > 101$, $M(n)$ is well defined because it equals $n - 10$. ■

Example 5.9.8 **The Ackermann Function**

Paul Fearn/Alamy Stock Photo

Wilhelm Ackermann (1896–1962)

In the 1920s the German logician and mathematician Wilhelm Ackermann first defined a version of the function that now bears his name. This function is important because its values are computable but cannot be evaluated using only for-next loops. The function is defined on the set of all pairs of nonnegative integers as follows:

$$A(0, n) = n + 1 \qquad \text{for all nonnegative integers } n \qquad 5.9.1$$

$$A(m, 0) = A(m - 1, 1) \qquad \text{for all positive integers } m \qquad 5.9.2$$

$$A(m, n) = A(m - 1, A(m, n - 1)) \qquad \text{for all positive integers } m \text{ and } n \qquad 5.9.3$$

Find $A(1, 2)$.

Solution

$$\begin{aligned}
A(1, 2) &= A(0, A(1, 1)) && \text{by (5.9.3) with } m = 1 \text{ and } n = 2\\
&= A(0, A(0, A(1, 0))) && \text{by (5.9.3) with } m = 1 \text{ and } n = 1\\
&= A(0, A(0, A(0, 1))) && \text{by (5.9.2) with } m = 1\\
&= A(0, A(0, 2)) && \text{by (5.9.1) with } n = 1\\
&= A(0, 3) && \text{by (5.9.1) with } n = 2\\
&= 4 && \text{by (5.9.1) with } n = 3.
\end{aligned}$$

The special properties of the Ackermann function are a consequence of its phenomenal rate of growth. While the values of $A(0, 0) = 1$, $A(1, 1) = 3$, $A(2, 2) = 7$, and $A(3, 3) = 61$ are not especially impressive,

$$A(4, 4) \cong 2^{2^{65536}}$$

and the values of $A(n, n)$ continue to increase with extraordinary rapidity thereafter. ■

The argument is somewhat technical, but it is not difficult to show that the Ackermann function is well defined. The following is an example of a recursive "definition" that does not define a function.

Example 5.9.9 **A Recursive "Function" That Is Not Well Defined**

Consider the following attempt to define a recursive function G from $\mathbf{Z}^+$ to $\mathbf{Z}$. For each integer $n \geq 1$,

$$G(n) = \begin{cases} 1 & \text{if } n \text{ is } 1 \\ 1 + G\left(\dfrac{n}{2}\right) & \text{if } n \text{ is even} \\ G(3n - 1) & \text{if } n \text{ is odd and } n > 1. \end{cases}$$

Is G well defined? Why?

Solution Suppose G is a function. Then by definition of G,

$$\begin{aligned}
&G(1) = 1,\\
&G(2) = 1 + G(1) = 1 + 1 = 2,\\
&G(3) = G(8) = 1 + G(4) = 1 + (1 + G(2)) = 1 + (1 + 2) = 4,\\
&G(4) = 1 + G(2) = 1 + 2 = 3.
\end{aligned}$$

However,

$$\begin{aligned}
G(5) &= G(14) = 1 + G(7) = 1 + G(20)\\
&= 1 + (1 + G(10)) = 1 + (1 + (1 + G(5))) = 3 + G(5).
\end{aligned}$$

Subtracting $G(5)$ from both sides gives $0 = 3$, which is false. Since the supposition that G is a function leads logically to a false statement, it follows that G is not a function. ■

A slight modification of the formula of Example 5.9.9 produces a "function" whose status of definition is unknown. Consider the following formula: For each integer $n \geq 1$,

$$T(n) = \begin{cases} 1 & \text{if } n \text{ is } 1 \\ T\left(\dfrac{n}{2}\right) & \text{if } n \text{ is even} \\ T(3n + 1) & \text{if } n \text{ is odd.} \end{cases}$$

In the 1930s, a student, Luther Collatz, became interested in the behavior of a related function g, which is defined as follows: $g(n) = n/2$ if n is even, and $g(n) = 3n + 1$ if n is odd. Collatz conjectured that for any initial positive number n, computation of successive values of $g(n)$, $g^2(n)$, $g^3(n)$, . . . would eventually produce the number 1. Determining whether this conjecture is true or false is called the **3*n* + 1 problem** (or the **3*x* + 1 problem**). If Collatz's conjecture is true, the formula for T defines a function; if the conjecture is false, T is not well defined. As of the publication of this book the answer is not known, although computer calculation has established that it holds for extremely large values of n.

TEST YOURSELF

1. The base for a recursive definition of a set is _____.
2. The recursion for a recursive definition of a set is _____.
3. The restriction for a recursive definition of a set is _____.
4. One way to show that a given element is in a recursively defined set is to start with an element or elements in the _____ and apply the rules from the _____ until you obtain the given element.
5. To use structural induction to prove that every element in a recursively defined set S satisfies a certain property, you show that _____ and that, for each rule in the recursion, if _____ then _____.
6. A function is said to be defined recursively if, and only if, _____.

EXERCISE SET 5.9

1. Consider the set of Boolean expressions defined in Example 5.9.1. Give derivations showing that each of the following is a Boolean expression over the English alphabet $\{a, b, c, \ldots, x, y, z\}$.
   a. $\sim p \vee (q \wedge (r \vee \sim s))$
   b. $(p \vee q) \vee \sim((p \wedge \sim s) \wedge r)$
2. Consider the set C of parenthesis structures defined in Example 5.9.2. Give derivations showing that each of the following is in C.
   a. ( )(( ))
   b. (( ))(( ))
3. Let S be the set of all strings over a finite set A and let a, b, and c be any characters in A.
   a. Using Theorem 5.9.1 but not Theorem 5.9.3 or 5.9.4, show that $(ab)c = a(bc)$.
   b. Show that ab is a string in S. Then use the result of part (a) to conclude that $a(bc)$ is a string in S.

   (This exercise shows that parentheses are not needed when writing the string abc.)
4. Consider the MIU-system discussed in Example 5.9.4. Give derivations showing that each of the following is in the MIU-system.
   a. $MIUI$
   b. $MUIIU$
5. The set of arithmetic expressions over the real numbers can be defined recursively as follows:
   I. Base: Each real number r is an arithmetic expression.
   II. Recursion: If u and v are arithmetic expressions, then the following are also arithmetic expressions:
   II(a) $(+u)$
   II(b) $(-u)$
   II(c) $(u + v)$
   II(d) $(u - v)$
   II(e) $(u \cdot v)$
   II(f) $\left(\frac{u}{v}\right)$
   III. Restriction: There are no arithmetic expressions over the real numbers other than those obtained from I and II.

   (Note that the *expression* $\left(\frac{u}{v}\right)$ is allowed to be an arithmetic expression even though the value of v may be 0.) Give derivations showing that each of the following is an arithmetic expression.
   a. $((2 \cdot (0.3–4.2)) + (-7))$ **b.** $\left(\frac{(9 \cdot (6 \cdot 1 + 2))}{((4 - 7) \cdot 6)}\right)$

6. Let S be a set of integers defined recursively as follows:

I. Base: 5 is in S.

II. Recursion: Given any integer n in S, $n + 4$ is in S.

III. Restriction: No integers are in S other than those derived from rules I and II above.

Use structural induction to prove that for every integer n in S, $n \bmod 2 = 1$.

7. Define a set S of strings over the set $\{0, 1\}$ recursively as follows:

I. Base: $1 \in S$

II. Recursion: If $s \in S$, then

II(a) $0s \in S$

II(b) $1s \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that every string in S ends in a 1.

8. Define a set S of strings over the set $\{a, b\}$ recursively as follows:

I. Base: $a \in S$

II. Recursion: If $s \in S$, then

II(a) $sa \in S$

II(b) $sb \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that every string in S begins with an a.

9. Define a set S of strings over the set $\{a, b\}$ recursively as follows:

I. Base: $\lambda \in S$

II. Recursion: If $s \in S$, then

II(a) $bs \in S$

II(b) $sb \in S$

II(c) $saa \in S$

II(d) $aas \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that every string in S contains an even number of a's.

10. Define a set S of strings over the set of all integers recursively as follows:

I. Base: $1 \in S$, $2 \in S$, $3 \in S$, $4 \in S$, $5 \in S$, $6 \in S$, $7 \in S$, $8 \in S$, $9 \in S$

II. Recursion: If $s \in S$ and $t \in S$, then

II(a) $s0 \in S$

II(b) $st \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that no string in S represents an integer with a leading zero.

***H* 11.** Define a set S of strings over the set of all integers recursively as follows:

I. Base: $1 \in S$, $3 \in S$, $5 \in S$, $7 \in S$, $9 \in S$

II. Recursion: If $s \in S$ and $t \in S$, then

II(a) $st \in S$

II(b) $2s \in S$

II(c) $4s \in S$

II(d) $6s \in S$

II(e) $8s \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that every string in S represents an odd integer when written in decimal notation.

***H* 12.** Define a set S of integers recursively as follows:

I. Base: $0 \in S$, $5 \in S$

II. Recursion: If $k \in S$ and $p \in S$, then

II(a) $k + p \in S$

II(b) $k - p \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that every integer in S is divisible by 5.

13. Define a set S of integers recursively as follows:

I. Base: $0 \in S$

II. Recursion: If $k \in S$, then

II(a) $k + 3 \in S$

II(b) $k - 3 \in S$

III. Restriction: Nothing is in S other than objects defined in I and II above.

Use structural induction to prove that every integer in S is divisible by 3.

***H* 14.** Is the string MU in the MIU-system? Use structural induction to prove your answer.

* **15.** Determine whether either of the following parenthesis configurations is in the set C defined in Example 5.9.2. Use structural induction to prove your answers.
a. ()(()
H **b.** (()()))(()

16. Give a recursive definition for the set of all strings of 0's and 1's that have the same number of 0's as 1's.

17. Give a recursive definition for the set of all strings of 0's and 1's for which all the 0's precede all the 1's.

18. Give a recursive definition for the set of all strings of a's and b's that contain an odd number of a's.

19. Give a recursive definition for the set of all strings of a's and b's that contain exactly one a.

20. **a.** Let A be any finite set and let L be the length function on the set of all strings over A. Prove that for every character a in A, $L(a) = 1$.
b. If A is a finite set, define a set S of strings over A as follows:

I. Base: Every character in A is a string in S.

II. Recursion: If s is any string in S, then for every character c in A, csc is a string in S.

III. Restriction: Nothing is in S except strings obtained from the base and the recursion.

Use structural induction to prove that given any string s in S, the length of s, $L(s)$, is an odd integer.

21. Write a complete proof for Theorem 5.9.4.

H **22.** If S is the set of all strings over a finite set A and if u is any string in S, define the *string reversal function*, Rev, as follows:
a. $\text{Rev}(\lambda) = \lambda$
b. For every string u in S and for every character a in A, $\text{Rev}(ua) = a\text{Rev}(u)$.
Use structural induction to prove that for all strings u and v in S, $\text{Rev}(uv) = \text{Rev}(v)\text{Rev}(u)$.

23. Use the definition of McCarthy's 91 function in Example 5.9.7 to show the following:
a. $M(86) = M(91)$
b. $M(91) = 91$

* **24.** Prove that McCarthy's 91 function equals 91 for all positive integers less than or equal to 101.

25. Use the definition of the Ackermann function in Example 5.9.8 to compute the following:
a. $A(1, 1)$
b. $A(2, 1)$

26. Use the definition of the Ackermann function to show the following:
a. $A(1, n) = n + 2$, for each nonnegative integer n
b. $A(2, n) = 3 + 2n$, for each nonnegative integer n
c. $A(3, n) = 8 \cdot 2^n - 3$, for each nonnegative integer n

27. Compute $T(2)$, $T(3)$, $T(4)$, $T(5)$, $T(6)$, and $T(7)$ for the "function" T defined after Example 5.9.9.

28. Student A tries to define a function $F : \mathbf{Z}^+ \to \mathbf{Z}$ by the rule

$$F(n) = \begin{cases} 1 & \text{if } n \text{ is } 1 \\ F\left(\dfrac{n}{2}\right) & \text{if } n \text{ is even} \\ 1 + F(5n - 9) & \text{if } n \text{ is odd and } n > 1 \end{cases}$$

for each integer $n \geq 1$. Student B claims that F is not well defined. Justify student B's claim.

29. Student C tries to define a function $G : \mathbf{Z}^+ \to \mathbf{Z}$ by the rule

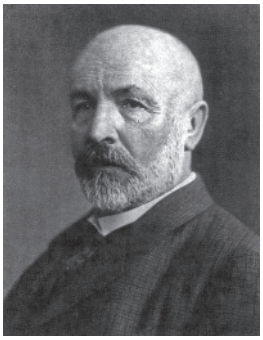
$$G(n) = \begin{cases} 1 & \text{if } n \text{ is } 1 \\ G\left(\dfrac{n}{2}\right) & \text{if } n \text{ is even} \\ 2 + G(3n - 5) & \text{if } n \text{ is odd and } n > 1 \end{cases}$$

for each integer $n \geq 1$. Student D claims that G is not well defined. Justify student D's claim.

ANSWERS FOR TEST YOURSELF

1. a statement that certain objects belong to the set **2.** a collection of rules indicating how to form new set objects from those already known to be in the set **3.** a statement that no objects belong to the set other than those coming from either the base or the recursion **4.** base; recursion **5.** each object in the base satisfies the property; the rule is applied to objects in the base; the objects defined by the rule also satisfy the property **6.** its rule of definition refers to itself

CHAPTER 6 SET THEORY



Pictorial Press Ltd./Alamy Stock Photo

Georg Cantor
(1845–1918)

In the late nineteenth century, Georg Cantor was the first to realize the potential usefulness of investigating properties of sets in general as distinct from properties of the elements that comprise them. Many mathematicians of his time resisted accepting the validity of Cantor's work. Now, however, abstract set theory is regarded as the foundation of mathematical thought. All mathematical objects (even numbers!) can be defined in terms of sets, and the language of set theory is used in every mathematical subject.

In this chapter we add to the basic definitions and notation of set theory introduced in Chapter 1 and show how to establish properties of sets through the use of proofs and counterexamples. We also introduce the notion of a Boolean algebra, explain how to derive its properties, and discuss their relationships to logical equivalencies and set identities. The chapter ends with a discussion of a famous "paradox" of set theory and its relation to computer science.

Source: David Eugene Smith Collection, Columbia University.

6.1 Set Theory: Definitions and the Element Method of Proof

The introduction of suitable abstractions is our only mental aid to organize and master complexity. —E. W. Dijkstra, 1930–2002

The words *set* and *element* are undefined terms of set theory just as *sentence*, *true*, and *false* are undefined terms of logic. The founder of set theory, Georg Cantor, suggested imagining a set as a "collection into a whole M of definite and separate objects of our intuition or our thought. These objects are called the elements of M." Cantor used the letter M because it is the first letter of the German word for set: *Menge*.

Following the spirit of Cantor's notation (though not the letter), let S denote a set and a an element of S. Then, as indicated in Section 1.2, $a \in S$ means that a is an element of S, $a \notin S$ means that a is not an element of S, $\{1, 2, 3\}$ refers to the set whose elements are 1, 2, and 3, and $\{1, 2, 3, \dots\}$ refers to the set of all positive integers. If S is a set and $P(x)$ is a property that elements of S may or may not satisfy, then a set A may be defined by writing

Caution! Don't forget to include the words "the set of all."

$$A = \{x \in S \mid P(x)\},$$

the set of all — such that

which is read "A is the set of all x in S such that P of x."

Subsets: Proof and Disproof

In Section 1.2 we defined what it means for a set A to be a subset of the set B. Here we rewrite the definition as a formal universal conditional statement:

$$A \subseteq B \iff \forall x, \text{ if } x \in A \text{ then } x \in B.$$

The negation is, therefore, existential:

$$A \not\subseteq B \iff \exists x \text{ such that } x \in A \text{ and } x \notin B.$$

Recall that a *proper subset* of a set is a subset that is not equal to its containing set. That is:

A is a **proper subset** of B $\iff$
(1) $A \subseteq B$, and
(2) there is at least one element in B that is not in A.

Example 6.1.1 **Testing Whether One Set Is a Subset of Another**

Let $A = \{1\}$ and $B = \{1, \{1\}\}$.

a. Is $A \subseteq B$?

b. If so, is A a proper subset of B?

Solution

a. Because $A = \{1\}$, A has only one element—namely, the symbol 1. This element is also one of the elements in set B. Hence every element in A is in B, and so $A \subseteq B$.

Note A set like $\{1\}$, with just one element, is called a **singleton set**.

b. B has two distinct elements, the symbol 1 and the set $\{1\}$ whose only element is 1. Since $1 \neq \{1\}$, the set $\{1\}$ is not an element of A, and so there is an element of B that is not an element of A. Hence A is a proper subset of B. ■

Because we define what it means for one set to be a subset of another by means of a universal conditional statement, we can use the method of direct proof to establish a subset relationship. Such a proof is called an *element argument* and is the fundamental proof technique of set theory.

Element Argument: The Basic Method for Proving That One Set Is a Subset of Another

Let sets X and Y be given. To prove that $X \subseteq Y$,

1. **suppose** that x is a particular but arbitrarily chosen element of X,
2. **show** that x is an element of Y.

Example 6.1.2 **Proving and Disproving Subset Relations**

Define sets A and B as follows:

$$A = \{m \in \mathbf{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbf{Z}\}$$
$$B = \{n \in \mathbf{Z} \mid n = 3s \text{ for some } s \in \mathbf{Z}\}.$$

a. Outline a proof that $A \subseteq B$. b. Prove that $A \subseteq B$. c. Disprove that $B \subseteq A$.

Solution

a. **Proof Outline:**
Starting Point: Suppose x is a particular but arbitrarily chosen element of A.

To Show: Therefore, x is an element of B.

b. **Proof:**
Suppose x is a particular but arbitrarily chosen element of A.

[We must show that $x \in B$. By definition of B, this means we must show that $x = 3\cdot$(some integer).]

By definition of A, there is an integer, say r, such that $x = 6r + 12$.

[Given that $x = 6r + 12$, can we express x as $3\cdot$(some integer)? That is, does $6r + 12 = 3\cdot$(some integer)? Yes, $6r + 12 = 3\cdot(2r + 4)$.]

Let $s = 2r + 4$.

[We must check that s is an integer.]

Then s is an integer because products and sums of integers are integers, and so $3s \in B$ by definition of B.

[Now we must check that $x = 3s$.]

Also $3s = 3(2r + 4) = 6r + 12 = x$,
Thus, by definition of B, x is an element of B,

[as was to be shown].

c. To disprove a statement means to show that it is false. And to show that $B \subseteq A$ is false, you must find an element of B that is not an element of A. By the definitions of A and B, this means that you must find an integer x of the form $3\cdot$(some integer) that cannot be written in the form $6\cdot$(some integer) $+ 12$. A little experimentation reveals that various numbers work. For instance, you could let $x = 3$. Then $x \in B$ because $3 = 3\cdot 1$, but $x \notin A$ because there is no integer r such that $3 = 6r + 12$. For if there were such an integer, then

Note Recall that the notation $P(x) \Rightarrow Q(x)$ means that every element that makes $P(x)$ true also makes $Q(x)$ true.

$$\begin{aligned} & 6r + 12 = 3 && \text{by assumption} \\ \Rightarrow\ & 2r + 4 = 1 && \text{by dividing both sides by 3} \\ \Rightarrow\ & 2r = -3 && \text{by subtracting 4 from both sides} \\ \Rightarrow\ & r = -3/2 && \text{by dividing both sides by 2.} \end{aligned}$$

But $-3/2$ is not an integer. Thus $3 \in B$ whereas $3 \notin A$, and so $B \not\subseteq A$. ■

Set Equality

Recall that by the axiom of extension, sets A and B are equal if, and only if, they have exactly the same elements. We restate this as a definition that uses the language of subsets.

Definition

Given sets A and B, A **equals** B, written $\boldsymbol{A = B}$, if, and only if, every element of A is in B and every element of B is in A.

Symbolically:

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ and } B \subseteq A.$$

This version of the definition of equality implies the following:

> To know that a set A equals a set B, you must know that $A \subseteq B$ and you must also know that $B \subseteq A$.

Example 6.1.3 **Set Equality**

Define sets A and B as follows:

$$A = \{m \in \mathbf{Z} \mid m = 2a \text{ for some integer } a\}$$

$$B = \{n \in \mathbf{Z} \mid n = 2b - 2 \text{ for some integer } b\}.$$

Is $A = B$?

Note A is the set of all integers that can be written as $2 \cdot$(some integer). The symbols m and a in the formal definition for A are used for convenience, but they can be replaced by any other symbols as long as the replacements are made consistently. For example, we can write

$A = \{n \in \mathbf{Z} \mid n = 2b$ for some integer $b\}$.

Solution Yes. To prove this, both subset relations $A \subseteq B$ and $B \subseteq A$ must be proved.

Part 1, Proof That $A \subseteq B$:

Suppose x is a particular but arbitrarily chosen element of A.

> *[We must show that $x \in B$. By definition of B, this means we must show that $x = 2 \cdot$(some integer) $- 2$.]*

By definition of A, there is an integer, say a, such that $x = 2a$.

> *[Given that $x = 2a$, can x also be expressed as $2 \cdot$(some integer) $- 2$? In other words, is there an integer—say, b—such that $2a = 2b - 2$? Solve for b to obtain $b = (2a + 2)/2 = a + 1$. Check to see if this works.]*

Let $b = a + 1$.

> *[First check that b is an integer.]*

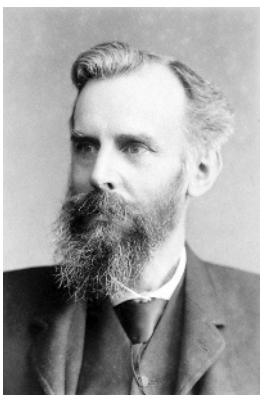
Then b is an integer because it is a sum of integers.

> *[Then check that $x = 2b - 2$.]*

Also, $2b - 2 = 2(a + 1) - 2 = 2a + 2 - 2 = 2a = x$.
Thus, by definition of B, x is an element of B

> *[as was to be shown].*

Part 2, Proof That $B \subseteq A$: This part of the proof is left as exercise 2 at the end of this section. ■

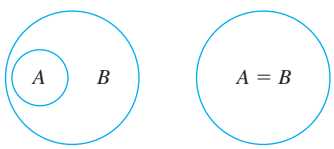


Pictures From History/Newscom

John Venn (1834–1923)

Venn Diagrams

If sets A and B are represented as regions in the plane, relationships between A and B can be represented by pictures called **Venn diagrams**, which were introduced by the British mathematician John Venn in 1881. For instance, the relationship $A \subseteq B$ can be pictured in one of two ways, as shown in Figure 6.1.1.



(a) (b)

FIGURE 6.1.1 $A \subseteq B$

The relationship $A \not\subseteq B$ can be represented in three different ways, as shown in Figure 6.1.2.

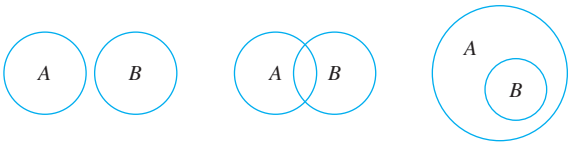


FIGURE 6.1.2 $A \not\subseteq B$

If we allow the possibility that some subregions of Venn diagrams do not contain any points, then in Figure 6.1.1 diagram (b) can be viewed as a special case of diagram (a) by imagining that the part of B outside A does not contain any points. Similarly, diagrams (a) and (c) of Figure 6.1.2 can be viewed as special cases of diagram (b). To obtain (a) from (b), imagine that the region of overlap between A and B does not contain any points. To obtain (c), imagine that the part of B that lies outside A does not contain any points. However, in all three diagrams it would be necessary to specify that there is a point in A that is not in B.

Example 6.1.4 **Relations among Sets of Numbers**

FIGURE 6.1.3

Since $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$ denote the sets of integers, rational numbers, and real numbers, respectively, then $\mathbf{Z}$ is a subset of $\mathbf{Q}$ because every integer is rational (any integer n can be written in the form $\frac{n}{1}$), and $\mathbf{Q}$ is a subset of $\mathbf{R}$ because every rational number is real (any rational number can be represented as a length on the number line). $\mathbf{Z}$ is a proper subset of $\mathbf{Q}$ because there are rational numbers that are not integers (for example, $\frac{1}{2}$), and $\mathbf{Q}$ is a proper subset of $\mathbf{R}$ because there are real numbers that are not rational (for example, $\sqrt{2}$). These relationships are shown diagrammatically in Figure 6.1.3. ■

Operations on Sets

Most mathematical discussions are carried on within some context. For example, in a certain situation all sets being considered might be sets of real numbers. In such a situation, the set of real numbers would be called a **universal set** or a **universe of discourse** for the discussion.

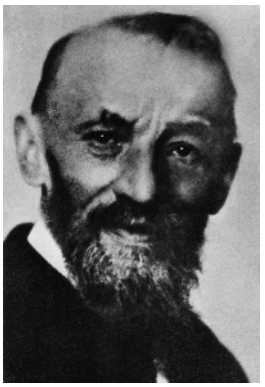
Definition

Let A and B be subsets of a universal set U.

1. The **union** of A and B, denoted $\boldsymbol{A \cup B}$, is the set of all elements that are in at least one of A or B.
2. The **intersection** of A and B, denoted $\boldsymbol{A \cap B}$, is the set of all elements that are common to both A and B.
3. The **difference** of B minus A (or **relative complement** of A in B), denoted $\boldsymbol{B - A}$, is the set of all elements that are in B and not A.
4. The **complement** of A, denoted $\boldsymbol{A^c}$, is the set of all elements in U that are not in A.

Symbolically:

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$
$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$
$$B - A = \{x \in U \mid x \in B \text{ and } x \notin A\}$$
$$A^c = \{x \in U \mid x \notin A\}.$$

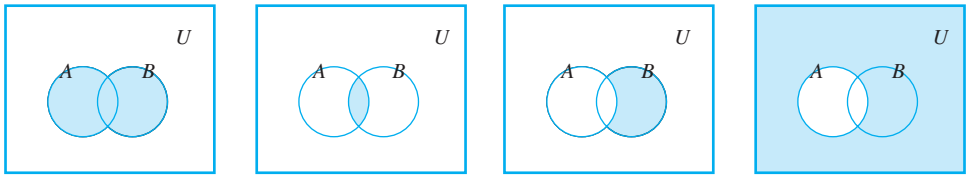


fototeca gilardi/Marka/Superstock

Giuseppe Peano (1858–1932)

The symbols ∈, ∪, and ∩ were introduced in 1889 by the Italian mathematician Giuseppe Peano.

Venn diagram representations for union, intersection, difference, and complement are shown in Figure 6.1.4.



Shaded region represents $A \cup B$.

Shaded region represents $A \cap B$.

Shaded region represents $B - A$.

Shaded region represents A^c.

FIGURE 6.1.4

Example 6.1.5 **Unions, Intersections, Differences, and Complements**

Let the universal set be the set $U = \{a, b, c, d, e, f, g\}$, and let $A = \{a, c, e, g\}$ and $B = \{d, e, f, g\}$. Find $A \cup B$, $A \cap B$, $B - A$, and A^c.

Solution

$$A \cup B = \{a, c, d, e, f, g\} \qquad A \cap B = \{e, g\}$$
$$B - A = \{d, f\} \qquad A^c = \{b, d, f\}$$

■

There is a convenient notation for subsets of real numbers that are intervals.

Interval Notation

Given real numbers a and b with $a \le b$:

$$(a, b) = \{x \in \mathbf{R} \mid a < x < b\} \qquad [a, b] = \{x \in \mathbf{R} \mid a \le x \le b\}$$
$$(a, b] = \{x \in \mathbf{R} \mid a < x \le b\} \qquad [a, b) = \{x \in \mathbf{R} \mid a \le x < b\}.$$

Note The symbol ∞ does not represent a number. It just indicates the unboundedness of the interval.

The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:

$$(a, \infty) = \{x \in \mathbf{R} \mid x > a\} \quad [a, \infty) = \{x \in \mathbf{R} \mid x \ge a\}$$
$$(-\infty, b) = \{x \in \mathbf{R} \mid x < b\} \quad (-\infty, b] = \{x \in \mathbf{R} \mid x \le b\}.$$

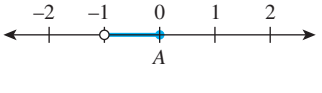
Although the notation for the interval (a, b) is identical to the notation for the ordered pair (a, b), context makes it unlikely that the two will be confused.

Example 6.1.6 **An Example with Intervals**

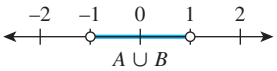
Let the universal set be $\mathbf{R}$, the set of all real numbers, and let

$$A = (-1, 0] = \{x \in \mathbf{R} \mid -1 < x \le 0\} \quad \text{and} \quad B = [0, 1) = \{x \in \mathbf{R} \mid 0 \le x < 1\}.$$

These sets are shown on the number lines below.

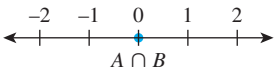


Find $A \cup B$, $A \cap B$, $B - A$, and A^c.

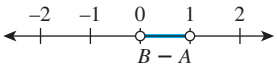


Solution

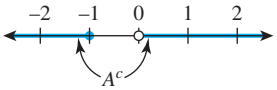
$A \cup B = \{x \in \mathbf{R} \mid x \in (-1, 0] \text{ or } x \in [0, 1)\} = \{x \in \mathbf{R} \mid x \in (-1, 1)\} = (-1, 1).$



$A \cap B = \{x \in \mathbf{R} \mid x \in (-1, 0] \text{ and } x \in [0, 1)\} = \{0\}.$



$B - A = \{x \in \mathbf{R} \mid x \in [0, 1) \text{ and } x \notin (-1, 0]\} = \{x \in \mathbf{R} \mid 0 < x < 1\} = (0, 1)$



$$\begin{aligned} A^c &= \{x \in \mathbf{R} \mid \text{it is not the case that } x \in (-1, 0]\} \\ &= \{x \in \mathbf{R} \mid \text{it is not the case that } (-1 < x \text{ and } x \le 0)\} && \text{by definition of the double inequality} \\ &= \{x \in \mathbf{R} \mid x \le -1 \text{ or } x > 0\} = (-\infty, -1] \cup (0, \infty) && \text{by De Morgan's law} \end{aligned}$$ ■

The definitions of unions and intersections for more than two sets are very similar to the definitions for two sets.

Definition

Unions and Intersections of an Indexed Collection of Sets

Given sets $A_0, A_1, A_2, \ldots$ that are subsets of a universal set U and given a nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i\}$$

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for every } i = 0, 1, 2, \ldots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for every nonnegative integer } i\}.$$

Note $\bigcup_{i=0}^{n} A_i$ is read "the union of the A-sub-i from i equals zero to n."

An alternative notation for $\bigcup_{i=0}^{n} A_i$ is $A_0 \cup A_1 \cup \ldots \cup A_n$, and an alternative notation for $\bigcap_{i=0}^{n} A_i$ is $A_0 \cap A_1 \cap \ldots \cap A_n$.

Example 6.1.7 **Finding Unions and Intersections of More than Two Sets**

For each positive integer i, let $A_i = \left\{x \in \mathbf{R} \mid -\frac{1}{i} < x < \frac{1}{i}\right\} = \left(-\frac{1}{i}, \frac{1}{i}\right)$.

a. Find $A_1 \cup A_2 \cup A_3$ and $A_1 \cap A_2 \cap A_3$. b. Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$.

Solution

a. $A_1 \cup A_2 \cup A_3 = \{x \in \mathbf{R} \mid x \text{ is in at least one of the intervals } (-1, 1),$

$\text{or } \left(-\frac{1}{2}, \frac{1}{2}\right), \text{ or } \left(-\frac{1}{3}, \frac{1}{3}\right)\}$

$$\begin{aligned} &= \{x \in \mathbf{R} \mid -1 < x < 1\} && \text{because all the elements in } \left(-\tfrac{1}{2}, \tfrac{1}{2}\right) \\ &= (-1, 1) && \text{and } \left(-\tfrac{1}{3}, \tfrac{1}{3}\right) \text{ are in } (-1, 1) \end{aligned}$$

$$A_1 \cap A_2 \cap A_3 = \left\{x \in \mathbf{R} \mid x \text{ is in all of the intervals } (-1, 1), \text{ and } \left(-\tfrac{1}{2}, \tfrac{1}{2}\right), \text{ and } \left(-\tfrac{1}{3}, \tfrac{1}{3}\right)\right\}$$
$$= \left\{x \in \mathbf{R} \mid -\tfrac{1}{3} < x < \tfrac{1}{3}\right\} \quad \text{because } \left(-\tfrac{1}{3}, \tfrac{1}{3}\right) \subseteq \left(-\tfrac{1}{2}, \tfrac{1}{2}\right) \subseteq (-1, 1)$$
$$= \left(-\tfrac{1}{3}, \tfrac{1}{3}\right)$$

b. $\bigcup_{i=1}^{\infty} A_i = \left\{x \in \mathbf{R} \mid x \text{ is in at least one of the intervals } \left(-\tfrac{1}{i}, \tfrac{1}{i}\right), \text{ where } i \text{ is a positive integer}\right\}$
$$= \{x \in \mathbf{R} \mid -1 < x < 1\} \quad \text{because all the elements in every interval } \left(-\tfrac{1}{i}, \tfrac{1}{i}\right) \text{ are in } (-1, 1)$$
$$= (-1, 1)$$

$$\bigcap_{i=1}^{\infty} A_i = \left\{x \in \mathbf{R} \mid x \text{ is in all of the intervals } \left(-\tfrac{1}{i}, \tfrac{1}{i}\right), \text{ where } i \text{ is a positive integer}\right\}$$
$$= \{0\} \quad \text{because the only element in every interval is 0}$$ ■

The Empty Set

We have stated that a set is defined by the elements that compose it. This being so, can there be a set that has no elements? It turns out that it is convenient to allow such a set. Otherwise, every time we wanted to take the intersection of two sets or to define a set by specifying a property, we would have to check that the result had elements and hence could be defined as a set. For example, if $A = \{1, 3\}$ and $B = \{2, 4\}$, then $A \cap B$ has no elements. Neither does $\{x \in \mathbf{R} \mid x^2 = -1\}$ because no real numbers have negative squares.

It may seem strange to talk about a set with no elements, but it often happens in mathematics that the definitions formulated to fit one set of circumstances are satisfied by some extreme cases not originally anticipated. Yet changing the definitions to exclude those cases would seriously undermine the simplicity and elegance of the theory taken as a whole.

In Section 6.2 we will show that there is only one set with no elements. Because it is unique, we can give it a special name. We call it the **empty set** (or **null set**) and denote it by the symbol $\varnothing$. Thus $\{1, 3\} \cap \{2, 4\} = \varnothing$ and $\{x \in \mathbf{R} \mid x^2 = -1\} = \varnothing$.

Example 6.1.8 **A Set with No Elements**

Describe the following sets.

a. $D = \{x \in \mathbf{R} \mid 3 < x < 2\}$.

b. $E = \{x \in \mathbf{Z} \mid 2 < x < 3\}$.

Solution:

a. Recall that $a < x < b$ means that $a < x$ and $x < b$. So D consists of all real numbers that are both greater than 3 and less than 2. Since there are no such numbers, D has no elements and thus $D = \varnothing$.

b. E is the set of all integers that are both greater than 2 and less than 3. Since no integers satisfy this condition, E has no elements, and so $E = \varnothing$. ■

Partitions of Sets

In many applications of set theory, sets are divided into nonoverlapping (or *disjoint*) pieces. Such a division is called a *partition*.

Definition

Two sets are called **disjoint** if, and only if, they have no elements in common.

Symbolically:

$$A \text{ and } B \text{ are disjoint} \iff A \cap B = \varnothing.$$

Example 6.1.9 **Disjoint Sets**

Let $A = \{1, 3, 5\}$ and $B = \{2, 4, 6\}$. Are A and B disjoint?

Solution Yes. By inspection A and B have no elements in common, or, in other words, $\{1, 3, 5\} \cap \{2, 4, 6\} = \varnothing$. ■

Definition

Sets $A_1, A_2, A_3, \ldots$ are **mutually disjoint** (or **pairwise disjoint** or **nonoverlapping**) if, and only if, no two sets A_i and A_j with distinct subscripts have any elements in common. More precisely, for all integers i and $j = 1, 2, 3, \ldots$

$$A_i \cap A_j = \varnothing \quad \text{whenever } i \neq j.$$

Example 6.1.10 **Mutually Disjoint Sets**

a. Let $A_1 = \{3, 5\}$, $A_2 = \{1, 4, 6\}$, and $A_3 = \{2\}$. Are A_1, A_2, and A_3 mutually disjoint?

b. Let $B_1 = \{2, 4, 6\}$, $B_2 = \{3, 7\}$, and $B_3 = \{4, 5\}$. Are B_1, B_2, and B_3 mutually disjoint?

Solution

a. Yes. A_1 and A_2 have no elements in common, A_1 and A_3 have no elements in common, and A_2 and A_3 have no elements in common.

b. No. B_1 and B_3 both contain 4. ■

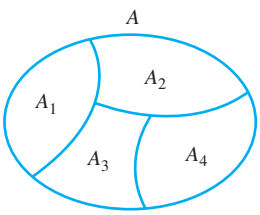


FIGURE 6.1.5 A Partition of a Set

Suppose A, A_1, A_2, A_3, and A_4 are the sets of points represented by the regions shown in Figure 6.1.5. Then A_1, A_2, A_3, and A_4 are subsets of A, and $A = A_1 \cup A_2 \cup A_3 \cup A_4$. Suppose further that boundaries are assigned to the regions representing A_1, A_2, A_3, and A_4 in such a way that these sets are mutually disjoint. Then A is called a *union of mutually disjoint subsets*, and the collection of sets $\{A_1, A_2, A_3, A_4\}$ is said to be a *partition* of A.

Definition

A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3, \ldots\}$ is a **partition** of a set A if, and only if,

1. A is the union of all the A_i;
2. the sets $A_1, A_2, A_3, \ldots$ are mutually disjoint.

Example 6.1.11 **Partitions of Sets**

a. Let $A = \{1, 2, 3, 4, 5, 6\}$, $A_1 = \{1, 2\}$, $A_2 = \{3, 4\}$, and $A_3 = \{5, 6\}$. Is $\{A_1, A_2, A_3\}$ a partition of A?

b. Let $\mathbf{Z}$ be the set of all integers and let

$$T_0 = \{n \in \mathbf{Z} \mid n = 3k, \text{ for some integer } k\},$$
$$T_1 = \{n \in \mathbf{Z} \mid n = 3k + 1, \text{ for some integer } k\}, \text{ and}$$
$$T_2 = \{n \in \mathbf{Z} \mid n = 3k + 2, \text{ for some integer } k\}.$$

Is $\{T_0, T_1, T_2\}$ a partition of $\mathbf{Z}$?

Solution

a. Yes. By inspection, $A = A_1 \cup A_2 \cup A_3$ and the sets A_1, A_2, and A_3 are mutually disjoint.

b. Yes. By the quotient-remainder theorem, every integer n can be represented in exactly one of the three forms

$$n = 3k \quad \text{or} \quad n = 3k + 1 \quad \text{or} \quad n = 3k + 2,$$

for some integer k. This implies that no integer can be in any two of the sets T_0, T_1, or T_2. So T_0, T_1, and T_2 are mutually disjoint. The theorem also implies that every integer is in one of the sets T_0, T_1, or T_2. So $\mathbf{Z} = T_0 \cup T_1 \cup T_2$. ■

Power Sets

There are various situations in which it is useful to consider the set of all subsets of a particular set. The **power set axiom** guarantees that this is a set.

Definition

Given a set A, the **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

Example 6.1.12 **Power Set of a Set**

Find the power set of the set $\{x, y\}$. That is, find $\mathcal{P}(\{x, y\})$.

Solution $\mathcal{P}(\{x, y\})$ is the set of all subsets of $\{x, y\}$. In Section 6.2 we will show that $\varnothing$ is a subset of every set, and so $\varnothing \in \mathcal{P}(\{x, y\})$. Also any set is a subset of itself, so $\{x, y\} \in \mathcal{P}(\{x, y\})$. The only other subsets of $\{x, y\}$ are $\{x\}$ and $\{y\}$, so

$$\mathcal{P}(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$$ ■

An Algorithm to Check Whether One Set Is a Subset of Another (Optional)

You may get some additional insight into the concept of subset by considering an algorithm for checking whether one finite set is a subset of another. Order the elements of both sets and successively compare each element of the first set with each element of the second set. If some element of the first set is not found to equal any element of the second, then the first set is not a subset of the second. But if each element of the first set is found to equal an element of the second set, then the first set is a subset of the second. The following algorithm formalizes this reasoning.

Algorithm 6.1.1 Testing Whether $A \subseteq B$

[The input sets A and B are represented as one-dimensional arrays a[1], a[2], . . . , a[m] and b[1], b[2], . . . , b[n], respectively. Starting with a[1] and for each successive a[i] in A, a check is made to see whether a[i] is in B. To do this, a[i] is compared to successive elements of B. If a[i] is not equal to any element of B, then the output string, called answer, is given the value "$A \not\subseteq B$." If a[i] equals some element of B, the next successive element in A is checked to see whether it is in B. If every successive element of A is found to be in B, then the answer never changes from its initial value "$A \subseteq B$."]

Input: *m [a positive integer], a[1], a[2], . . . , a[m] [a one-dimensional array representing the set A], n [a positive integer], b[1], b[2], . . . , b[n] [a one-dimensional array representing the set B]*

Algorithm Body:

$i := 1$, *answer* := "$A \subseteq B$"
while ($i \leq m$ and *answer* = "$A \subseteq B$")
  $j := 1$, *found* := "no"
    while ($j \leq n$ and *found* = "no")
      if $a[i] = b[j]$ **then** *found* := "yes"
      $j := j + 1$
    end while
    [If found has not been given the value "yes" when execution reaches this point, then $a[i] \notin B$.]
    if *found* = "no" **then** *answer* := "$A \not\subseteq B$"
    $i := i + 1$
end while

Output: *answer [a string]*

Example 6.1.13 **Tracing Algorithm 6.1.1**

Trace the action of Algorithm 6.1.1 on the variables i, j, *found*, and *answer* for $m = 3$, $n = 4$, and sets A and B represented as the arrays $a[1] = u$, $a[2] = v$, $a[3] = w$, $b[1] = w$, $b[2] = x$, $b[3] = y$, and $b[4] = u$.

Solution

i	1					2					3
j	1	2	3	4	5	1	2	3	4	5	
found	no			yes		no					
answer	$A \subseteq B$									$A \not\subseteq B$	

In the exercises at the end of this section, you are asked to write an algorithm to check whether a given element is in a given set. To do this, you can represent the set as a one-dimensional array and compare the given element with successive elements of the array to determine whether the two elements are equal. If they are, then the element is in the set; if the given element does not equal any element of the array, then the element is not in the set.

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. The notation $A \subseteq B$ is read "_____" and means that _____.
2. To use an element argument for proving that a set X is a subset of a set Y, you suppose that _____ and show that _____.
3. To disprove that a set X is a subset of a set Y, you show that there is _____.
4. An element x is in $A \cup B$ if, and only if, _____.
5. An element x is in $A \cap B$ if, and only if, _____.
6. An element x is in $B - A$ if, and only if, _____.
7. An element x is in A^c if, and only if, _____.
8. The empty set is a set with _____.
9. The power set of a set A is _____.
10. Sets A and B are disjoint if, and only if, _____.
11. A collection of nonempty sets $A_1, A_2, A_3, \ldots$ is a partition of a set A if, and only if, _____.

EXERCISE SET 6.1*

1. In each of (a)–(f), answer the following questions: Is $A \subseteq B$? Is $B \subseteq A$? Is either A or B a proper subset of the other?
   a. $A = \{2, \{2\}, (\sqrt{2})^2\}$, $B = \{2, \{2\}, \{\{2\}\}\}$
   b. $A = \{3, \sqrt{5^2 - 4^2}, 24 \bmod 7\}$, $B = \{8 \bmod 5\}$
   c. $A = \{\{1, 2\}, \{2, 3\}\}$, $B = \{1, 2, 3\}$
   d. $A = \{a, b, c\}$, $B = \{\{a\}, \{b\}, \{c\}\}$
   e. $A = \{\sqrt{16}, \{4\}\}$, $B = \{4\}$
   f. $A = \{x \in \mathbf{R} \mid \cos x \in \mathbf{Z}\}$, $B = \{x \in \mathbf{R} \mid \sin x \in \mathbf{Z}\}$
2. Complete the proof from Example 6.1.3: Prove that $B \subseteq A$ where
   $$A = \{m \in \mathbf{Z} \mid m = 2a \text{ for some integer } a\}$$
   and
   $$B = \{n \in \mathbf{Z} \mid n = 2b - 2 \text{ for some integer } b\}$$
3. Let sets R, S, and T be defined as follows:
   $$R = \{x \in \mathbf{Z} \mid x \text{ is divisible by } 2\}$$
   $$S = \{y \in \mathbf{Z} \mid y \text{ is divisible by } 3\}$$
   $$T = \{z \in \mathbf{Z} \mid z \text{ is divisible by } 6\}.$$
   Prove or disprove each of the following statements.
   a. $R \subseteq T$ b. $T \subseteq R$ c. $T \subseteq S$
4. Let $A = \{n \in \mathbf{Z} \mid n = 5r \text{ for some integer } r\}$ and $B = \{m \in \mathbf{Z} \mid m = 20s \text{ for some integer } s\}$. Prove or disprove each of the following statements.
   a. $A \subseteq B$ b. $B \subseteq A$
5. Let $C = \{n \in \mathbf{Z} \mid n = 6r - 5 \text{ for some integer } r\}$ and $D = \{m \in \mathbf{Z} \mid m = 3s + 1 \text{ for some integer } s\}$.
   Prove or disprove each of the following statements.
   a. $C \subseteq D$ b. $D \subseteq C$
6. Let $A = \{x \in \mathbf{Z} \mid x = 5a + 2 \text{ for some integer } a\}$, $B = \{y \in \mathbf{Z} \mid y = 10b - 3 \text{ for some integer } b\}$, and $C = \{z \in \mathbf{Z} \mid z = 10c + 7 \text{ for some integer } c\}$.
   Prove or disprove each of the following statements.
   a. $A \subseteq B$ b. $B \subseteq A$ H c. $B = C$
7. Let $A = \{x \in \mathbf{Z} \mid x = 6a + 4 \text{ for some integer } a\}$, $B = \{y \in \mathbf{Z} \mid y = 18b - 2 \text{ for some integer } b\}$, and $C = \{z \in \mathbf{Z} \mid z = 18c + 16 \text{ for some integer } c\}$.
   Prove or disprove each of the following statements.
   a. $A \subseteq B$ b. $B \subseteq A$ c. $B = C$
8. Write in words how to read each of the following out loud. Then write each set using the symbols for union, intersection, set difference, or set complement.
   a. $\{x \in U \mid x \in A \text{ and } x \in B\}$
   b. $\{x \in U \mid x \in A \text{ or } x \in B\}$
   c. $\{x \in U \mid x \in A \text{ and } x \notin B\}$
   d. $\{x \in U \mid x \notin A\}$
9. Complete the following sentences without using the symbols $\cup$, $\cap$, or $-$.
   a. $x \notin A \cup B$ if, and only if, _____.
   b. $x \notin A \cap B$ if, and only if, _____.
   c. $x \notin A - B$ if, and only if, _____.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol H indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

10. Let $A = \{1, 3, 5, 7, 9\}$, $B = \{3, 6, 9\}$, and $C = \{2, 4, 6, 8\}$. Find each of the following:
a. $A \cup B$ **b.** $A \cap B$ **c.** $A \cup C$ **d.** $A \cap C$
e. $A - B$ **f.** $B - A$ **g.** $B \cup C$ **h.** $B \cap C$

11. Let the universal set be $\mathbf{R}$, the set of all real numbers, and let $A = \{x \in \mathbf{R} \mid 0 < x \leq 2\}$, $B = \{x \in \mathbf{R} \mid 1 \leq x < 4\}$, and $C = \{x \in \mathbf{R} \mid 3 \leq x < 9\}$. Find each of the following:
a. $A \cup B$ **b.** $A \cap B$ **c.** A^c **d.** $A \cup C$
e. $A \cap C$ **f.** B^c **g.** $A^c \cap B^c$
h. $A^c \cup B^c$ **i.** $(A \cap B)^c$ **j.** $(A \cup B)^c$

12. Let the universal set be $\mathbf{R}$, the set of all real numbers, and let $A = \{x \in \mathbf{R} \mid -3 \leq x \leq 0\}$, $B = \{x \in \mathbf{R} \mid -1 < x < 2\}$, and $C = \{x \in \mathbf{R} \mid 6 < x \leq 8\}$. Find each of the following:
a. $A \cup B$ **b.** $A \cap B$ **c.** A^c **d.** $A \cup C$
e. $A \cap C$ **f.** B^c **g.** $A^c \cap B^c$
h. $A^c \cup B^c$ **i.** $(A \cap B)^c$ **j.** $(A \cup B)^c$

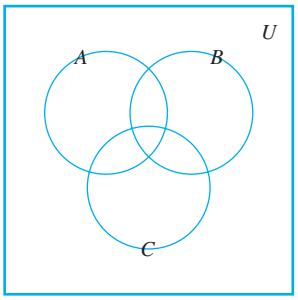
13. Let S be the set of all strings of 0's and 1's of length 4, and let A and B be the following subsets of S: $A = \{1110, 1111, 1000, 1001\}$ and $B = \{1100, 0100, 1111, 0111\}$. Find each of the following:
a. $A \cap B$ **b.** $A \cup B$ **c.** $A - B$ **d.** $B - A$

14. In each of the following, draw a Venn diagram for sets A, B, and C that satisfy the given conditions.
a. $A \subseteq B$, $C \subseteq B$, $A \cap C = \emptyset$
b. $C \subseteq A$, $B \cap C = \emptyset$

15. In each of the following, draw a Venn diagram for sets A, B, and C that satisfy the given conditions.
a. $A \cap B = \emptyset$, $A \subseteq C$, $C \cap B \neq \emptyset$
b. $A \subseteq B$, $C \subseteq B$, $A \cap C \neq \emptyset$
c. $A \cap B \neq \emptyset$, $B \cap C \neq \emptyset$, $A \cap C = \emptyset$, $A \not\subseteq B$, $C \not\subseteq B$

16. Let $A = \{a, b, c\}$, $B = \{b, c, d\}$, and $C = \{b, c, e\}$.
a. Find $A \cup (B \cap C)$, $(A \cup B) \cap C$, and $(A \cup B) \cap (A \cup C)$. Which of these sets are equal?
b. Find $A \cap (B \cup C)$, $(A \cap B) \cup C$, and $(A \cap B) \cup (A \cap C)$. Which of these sets are equal?
c. Find $(A - B) - C$ and $A - (B - C)$. Are these sets equal?

17. Consider the following Venn diagram. For each of (a)–(f), copy the diagram and shade the region corresponding to the indicated set.
a. $A \cap B$ **b.** $B \cup C$ **c.** A^c
d. $A - (B \cup C)$ **e.** $(A \cup B)^c$ **f.** $A^c \cap B^c$



18. **a.** Is the number 0 in $\emptyset$? Why?
b. Is $\emptyset = \{\emptyset\}$? Why?
c. Is $\emptyset \in \{\emptyset\}$? Why?
d. Is $\emptyset \in \emptyset$? Why?

19. Let $A_i = \{i, i^2\}$ for each integer $i = 1, 2, 3, 4$.
a. $A_1 \cup A_2 \cup A_3 \cup A_4 = ?$
b. $A_1 \cap A_2 \cap A_3 \cap A_4 = ?$
c. Are A_1, A_2, A_3, and A_4 mutually disjoint? Explain.

20. Let $B_i = \{x \in \mathbf{R} \mid 0 \leq x \leq i\}$ for each integer $i = 1, 2, 3, 4$.
a. $B_1 \cup B_2 \cup B_3 \cup B_4 = ?$
b. $B_1 \cap B_2 \cap B_3 \cap B_4 = ?$
c. Are B_1, B_2, B_3, and B_4 mutually disjoint? Explain.

21. Let $C_i = \{i, -i\}$ for each nonnegative integer i.
a. $\bigcup_{i=0}^{4} C_i = ?$ **b.** $\bigcap_{i=0}^{4} C_i = ?$
c. Are C_0, C_1, C_2, ... mutually disjoint? Explain.
d. $\bigcup_{i=0}^{n} C_i = ?$ **e.** $\bigcap_{i=0}^{n} C_i = ?$
f. $\bigcup_{i=0}^{\infty} C_i = ?$ **g.** $\bigcap_{i=0}^{\infty} C_i = ?$

22. Let $D_i = \{x \in \mathbf{R} \mid -i \leq x \leq i\} = [-i, i]$ for each nonnegative integer i.
a. $\bigcup_{i=0}^{4} D_i = ?$ **b.** $\bigcap_{i=0}^{4} D_i = ?$
c. Are D_0, D_1, D_2, ... mutually disjoint? Explain.
d. $\bigcup_{i=0}^{n} D_i = ?$ **e.** $\bigcap_{i=0}^{n} D_i = ?$
f. $\bigcup_{i=0}^{\infty} D_i = ?$ **g.** $\bigcap_{i=0}^{\infty} D_i = ?$

23. Let $V_i = \left\{x \in \mathbf{R} \mid -\frac{1}{i} \leq x \leq \frac{1}{i}\right\} = \left[-\frac{1}{i}, \frac{1}{i}\right]$ for each positive integer i.
a. $\bigcup_{i=0}^{4} V_i = ?$ **b.** $\bigcap_{i=0}^{4} V_i = ?$

c. Are $V_1, V_2, V_3, \ldots$ mutually disjoint? Explain.

d. $\bigcup_{i=0}^{n} V_i = ?$ **e.** $\bigcap_{i=0}^{n} V_i = ?$

f. $\bigcup_{i=0}^{\infty} V_i = ?$ **g.** $\bigcap_{i=0}^{\infty} V_i = ?$

24. Let $W_i = \{x \in \mathbf{R} \mid x > i\} = (i, \infty)$ for each nonnegative integer i.

a. $\bigcup_{i=0}^{4} W_i = ?$ **b.** $\bigcap_{i=0}^{4} W_i = ?$

c. Are $W_0, W_1, W_2, \ldots$ mutually disjoint? Explain.

d. $\bigcup_{i=0}^{n} W_i = ?$ **e.** $\bigcap_{i=0}^{n} W_i = ?$

f. $\bigcup_{i=0}^{\infty} W_i = ?$ **g.** $\bigcap_{i=0}^{\infty} W_i = ?$

25. Let $R_i = \left\{x \in \mathbf{R} \mid 1 \le x \le 1 + \frac{1}{i}\right\} = \left[1, 1 + \frac{1}{i}\right]$ for each positive integer i.

a. $\bigcup_{i=0}^{4} R_i = ?$ **b.** $\bigcap_{i=0}^{4} R_i = ?$

c. Are $R_1, R_2, R_3, \ldots$ mutually disjoint? Explain.

d. $\bigcup_{i=0}^{n} R_i = ?$ **e.** $\bigcap_{i=0}^{n} R_i = ?$

f. $\bigcup_{i=0}^{\infty} R_i = ?$ **g.** $\bigcap_{i=0}^{\infty} R_i = ?$

26. Let $S_i = \left\{x \in \mathbf{R} \mid 1 < x < 1 + \frac{1}{i}\right\} = \left(1, 1 + \frac{1}{i}\right)$ for each positive integer i.

a. $\bigcup_{i=0}^{4} S_i = ?$ **b.** $\bigcap_{i=0}^{4} S_i = ?$

c. Are $S_1, S_2, S_3, \ldots$ mutually disjoint? Explain.

d. $\bigcup_{i=0}^{n} S_i = ?$ **e.** $\bigcap_{i=0}^{n} S_i = ?$

f. $\bigcup_{i=0}^{\infty} S_i = ?$ **g.** $\bigcap_{i=0}^{\infty} S_i = ?$

27. a. Is $\{\{a, d, e\}, \{b, c\}, \{d, f\}\}$ a partition of $\{a, b, c, d, e, f\}$?

b. Is $\{\{w, x, v\}, \{u, y, q\}, \{p, z\}\}$ a partition of $\{p, q, u, v, w, x, y, z\}$?

c. Is $\{\{5, 4\}, \{7, 2\}, \{1, 3, 4\}, \{6, 8\}\}$ a partition of $\{1, 2, 3, 4, 5, 6, 7, 8\}$?

d. Is $\{\{3, 7, 8\}, \{2, 9\}, \{1, 4, 5\}\}$ a partition of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$?

e. Is $\{\{1, 5\}, \{4, 7\}, \{2, 8, 6, 3\}\}$ a partition of $\{1, 2, 3, 4, 5, 6, 7, 8\}$?

28. Let E be the set of all even integers and O the set of all odd integers. Is $\{E, O\}$ a partition of $\mathbf{Z}$, the set of all integers? Explain your answer.

29. Let $\mathbf{R}$ be the set of all real numbers. Is $\{\mathbf{R}^+, \mathbf{R}^-, \{0\}\}$ a partition of $\mathbf{R}$? Explain your answer.

30. Let $\mathbf{Z}$ be the set of all integers and let

$$A_0 = \{n \in \mathbf{Z} \mid n = 4k, \text{ for some integer } k\}$$
$$A_1 = \{n \in \mathbf{Z} \mid n = 4k + 1, \text{ for some integer } k\}$$
$$A_2 = \{n \in \mathbf{Z} \mid n = 4k + 2, \text{ for some integer } k\}$$

and

$$A_3 = \{n \in \mathbf{Z} \mid n = 4k + 3, \text{ for some integer } k\}.$$

Is $\{A_0, A_1, A_2, A_3\}$ a partition of $\mathbf{Z}$? Explain your answer.

31. Suppose $A = \{1, 2\}$ and $B = \{2, 3\}$. Find each of the following:

a. $\mathcal{P}(A \cap B)$

b. $\mathcal{P}(A)$

c. $\mathcal{P}(A \cup B)$

d. $\mathcal{P}(A \times B)$

32. a. Suppose $A = \{1\}$ and $B = \{u, v\}$. Find $\mathcal{P}(A \times B)$.

b. Suppose $X = \{a, b\}$ and $Y = \{x, y\}$. Find $\mathcal{P}(X \times Y)$.

33. a. Find $\mathcal{P}(\varnothing)$. **b.** Find $\mathcal{P}(\mathcal{P}(\varnothing))$.

c. Find $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$.

34. Let $A_1 = \{1\}$, $A_2 = \{u, v\}$, and $A_3 = \{m, n\}$. Find each of the following sets:

a. $A_1 \cup (A_2 \times A_3)$

b. $(A_1 \cup A_2) \times A_3$

35. Let $A = \{a, b\}$, $B = \{1, 2\}$, and $C = \{2, 3\}$. Find each of the following sets.

a. $A \times (B \cup C)$ **b.** $(A \times B) \cup (A \times C)$

c. $A \times (B \cap C)$ **d.** $(A \times B) \cap (A \times C)$

36. Trace the action of Algorithm 6.1.1 on the variables i, j, *found*, and *answer* for $m = 3$, $n = 3$, and sets A and B represented as the arrays $a[1] = u$, $a[2] = v$, $a[3] = w$, $b[1] = w$, $b[2] = u$, and $b[3] = v$.

37. Trace the action of Algorithm 6.1.1 on the variables i, j, *found*, and *answer* for $m = 4$, $n = 4$, and sets A and B represented as the arrays $a[1] = u$, $a[2] = v$, $a[3] = w$, $a[4] = x$, $b[1] = r$, $b[2] = u$, $b[3] = y$, $b[4] = z$.

38. Write an algorithm to determine whether a given element x belongs to a given set that is represented as the array $a[1], a[2], \ldots, a[n]$.

ANSWERS FOR TEST YOURSELF

1. the set A is a subset of the set B; for every x, if $x \in A$ then $x \in B$ (*Or:* every element of A is also an element of B) **2.** x is any *[particular but arbitrarily chosen]* element of X; x is an element of Y **3.** an element in X that is not in Y **4.** x is in A or x is in B (*Or:* x is in at least one of the sets A and B) **5.** x is in A and x is in B (*Or:* x is in both A and B) **6.** x is in B and x is not in A **7.** x is in the universal set and is not in A **8.** no elements **9.** the set of all subsets of A **10.** $A \cap B = \emptyset$ (*Or:* A and B have no elements in common) **11.** A is the union of all the sets $A_1, A_2, A_3, \ldots$ and $A_i \cap A_j = \emptyset$ whenever $i \neq j$

6.2 Properties of Sets

. . . only the last line is a genuine theorem here—everything else is in the fantasy.
—Douglas Hofstadter, *Gödel, Escher, Bach*, 1979

It is possible to list many relations involving unions, intersections, complements, and differences of sets. Some of these are true for all sets, whereas others fail to hold in some cases. In this section we show how to establish basic set properties using *element arguments*, and we discuss a variation used to prove that a set is empty. In the next section we will show how to disprove a proposed set property by constructing a counterexample and how to use an algebraic technique to derive new set properties from set properties already known to be true.

We begin by listing some set properties that involve subset relations. As you read them, keep in mind that the operations of union, intersection, and difference take precedence over set inclusion. Thus, for example, $A \cap B \subseteq C$ means $(A \cap B) \subseteq C$.

Theorem 6.2.1 Some Subset Relations

1. *Inclusion of Intersection:* For all sets A and B,

$$\text{(a) } A \cap B \subseteq A \quad \text{and} \quad \text{(b) } A \cap B \subseteq B.$$

2. *Inclusion in Union:* For all sets A and B,

$$\text{(a) } A \subseteq A \cup B \quad \text{and} \quad \text{(b) } B \subseteq A \cup B.$$

3. *Transitive Property of Subsets:* For all sets A, B, and C,

$$\text{if } A \subseteq B \text{ and } B \subseteq C, \text{ then } A \subseteq C.$$

The conclusion of each part of Theorem 6.2.1 states that one set X is a subset of another set Y and so to prove them, you suppose that x is any *[particular but arbitrarily chosen]* element of X, and you show that x is an element of Y.

In most proofs of set properties, the secret of getting from the assumption that x is in X to the conclusion that x is in Y is to think of the definitions of basic set operations in terms of how they act on elements, that is, in procedural terms. For example, the union of sets X and Y, $X \cup Y$, is defined as

$$X \cup Y = \{x \mid x \in X \quad \text{or} \quad x \in Y\}.$$

This means that any time you know an element x is in $X \cup Y$, you can conclude that x must be in X *or* x must be in Y. Conversely, any time you know that a particular x is in some set X or is in some set Y, you can conclude that x is in $X \cup Y$. Thus, for any sets X and Y and any element x,

$$x \in X \cup Y \quad \text{if, and only if,} \quad x \in X \quad \text{or} \quad x \in Y.$$

Procedural versions of the definitions of the other set operations are derived similarly and are summarized below.

Procedural Versions of Set Definitions

Let X and Y be subsets of a universal set U and suppose x and y are elements of U.

1. $x \in X \cup Y \iff x \in X$ or $x \in Y$
2. $x \in X \cap Y \iff x \in X$ and $x \in Y$
3. $x \in X - Y \iff x \in X$ and $x \notin Y$
4. $x \in X^c \iff x \notin X$
5. $(x, y) \in X \times Y \iff x \in X$ and $y \in Y$

Proving a Subset Relation

Consider trying to prove Theorem 6.2.1(a): For all sets A and B, $A \cap B \subseteq A$. First notice that the statement is universal. It makes a claim about *all* sets A and B. So the proof has the following outline:

Starting Point: Suppose A and B are any *[particular but arbitrarily chosen]* sets.

To Show: $A \cap B \subseteq A$

Now to prove $A \cap B \subseteq A$ you must use the definition of subset. In other words, you must show that

$$\forall x, \text{ if } x \in A \cap B, \text{ then } x \in A.$$

This statement is also universal, and to prove it you use an element argument:

suppose x is any element in $A \cap B$

and

show that x is in A.

You can fill in the gap between "suppose" and the "show" by using the procedural version of the definition of intersection along with your knowledge of logic and the definition of subset. Examples 6.2.1(a) and 6.2.1(b) show proofs for Theorem 6.2.1(1)(a) and Theorem 6.2.1(2)(a). Each contains blanks to fill in with explanations or parts of proof steps.

Example 6.2.1 **Fill in the Blanks for Proofs of Subset Relations**

Fill in the blanks in the proofs shown below.

a. **Theorem 6.2.1(1)(a):** For all sets A and B, $A \cap B \subseteq A$.
Proof:

Statement	Explanation
Suppose A and B are any sets.	starting point
We must show that $A \cap B \subseteq A$.	conclusion to be shown
Let x be any element in $A \cap B$.	start of an element argument
Then x is in A and x is in B.	_____(*i*)_____
In particular, x is in A.	_____(*ii*)_____
Thus every element in $A \cap B$ is in A.	because x could be any element of $A \cap B$
Therefore, $A \cap B \subseteq A$.	_____(*iii*)_____

b. **Theorem 6.2.1(2)(a):** For all sets A and B, $A \subseteq A \cup B$.
Proof:

Statement	Explanation
Suppose __(i)__.	starting point
We must show that $A \subseteq A \cup B$.	conclusion to be shown
__(ii)__	start of an element argument
Then the following statement is true: "x is in A or x is in B."	For an *or* statement to be true only __(iii)__ component needs to be true.
Thus x is in $A \cup B$.	by definition of union
Hence every element in A is in __(iv)__.	because x could be any element of A
Therefore, __(v)__.	by definition of subset

Solution

a. (*i*) by definition of intersection (*ii*) If an *and* statement is true, then each individual component is true. (*iii*) by definition of subset

b. (*i*) A and B are any sets. (*ii*) Let x be any element in A. (*Or: Suppose x is any element in A.*) (*iii*) one (*iv*) $A \cup B$ (*v*) $A \subseteq A \cup B$ ■

In his book *Gödel, Escher, Bach*,* Douglas Hofstadter introduces the fantasy rule for mathematical proof. Hofstadter points out that when you start a mathematical argument with *if*, *let*, or *suppose*, you are stepping into a fantasy world where not only are all the facts of the real world true but whatever you are supposing is also true. Once you are in that world, you can suppose something else. That sends you into a subfantasy world where not only is everything in the fantasy world true but also the new thing you are supposing. Of course, you can continue stepping into new subfantasy worlds in this way indefinitely. You return one level closer to the real world each time you derive a conclusion that makes a whole if-then or universal statement true. Your aim in a proof is to continue deriving such conclusions until you return to the world from which you made your first supposition.

Occasionally, mathematical problems are stated in the following form:

> Suppose (*statement* 1). Prove that (*statement* 2).

When this phrasing is used, the author intends the reader to add statement 1 to his or her general mathematical knowledge and not to make explicit reference to it in the proof. In Hofstadter's terms, the author invites the reader to enter a fantasy world where statement 1 is known to be true and to prove statement 2 in this fantasy world. Thus the solver of such a problem would begin a proof with the starting point for a proof of statement 2. Consider, for instance, the following restatement from Example 6.2.1(a):

> Suppose A and B are arbitrarily chosen sets.
>
> Prove that $A \cap B \subseteq A$.

The proof would begin "Suppose $x \in A \cap B$," it being *understood* that sets A and B have already been chosen arbitrarily.

The proofs in Example 6.2.1 are called element arguments because they show one set to be a subset of another by demonstrating that every element in the one set is also an element in the other. In higher mathematics, element arguments are the standard method for establishing relations among sets. High-school students are often allowed to justify set properties

**Gödel, Escher, Bach: An Eternal Golden Braid* (New York: Basic Books, 1979).

by using Venn diagrams. This method is appealing, but for it to be mathematically rigorous may be more complicated than you might expect. Appropriate Venn diagrams can be drawn for two or three sets, but the verbal explanations needed to justify conclusions inferred from them are normally as long or longer than a straightforward element proof.

In general, Venn diagrams are not very helpful when the number of sets is four or more. For instance, if the requirement is made that a Venn diagram must show every possible intersection of the sets, it is impossible to draw a symmetric Venn diagram for four sets, or, in fact, for any nonprime number of sets. In 2002, computer scientists/mathematicians Carla Savage and Jerrold Griggs and undergraduate student Charles Killian solved a long-standing open problem by proving that it *is* possible to draw such a symmetric Venn diagram for any prime number of sets. For $n > 5$, however, the resulting pictures are extremely complicated! However, the fact that such symmetric diagrams exist has applications in the area of computer science called coding theory.

Set Identities

An **identity** is an equation that is universally true for all elements in some set. For example, the equation $a + b = b + a$ is an identity for real numbers because it is true for all real numbers a and b. The collection of set properties in the next theorem consists entirely of set identities. That is, they are equations that are true for all sets in some universal set.

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,
$$\text{(a) } A \cup B = B \cup A \quad \text{and} \quad \text{(b) } A \cap B = B \cap A.$$
2. *Associative Laws:* For all sets A, B, and C,
$$\text{(a) } (A \cup B) \cup C = A \cup (B \cup C) \quad \text{and}$$
$$\text{(b) } (A \cap B) \cap C = A \cap (B \cap C).$$
3. *Distributive Laws:* For all sets A, B, and C,
$$\text{(a) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and}$$
$$\text{(b) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
4. *Identity Laws:* For every set A,
$$\text{(a) } A \cup \varnothing = A \quad \text{and} \quad \text{(b) } A \cap U = A.$$
5. *Complement Laws:* For every set A,
$$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \varnothing.$$
6. *Double Complement Law:* For every set A,
$$(A^c)^c = A.$$
7. *Idempotent Laws:* For every set A,
$$\text{(a) } A \cup A = A \quad \text{and} \quad \text{(b) } A \cap A = A.$$

8. *Universal Bound Laws:* For every set A,
$$\text{(a) } A \cup U = U \quad \text{and} \quad \text{(b) } A \cap \varnothing = \varnothing.$$
9. *De Morgan's Laws:* For all sets A and B,
$$\text{(a) } (A \cup B)^c = A^c \cap B^c \quad \text{and} \quad \text{(b) } (A \cap B)^c = A^c \cup B^c.$$
10. *Absorption Laws:* For all sets A and B,
$$\text{(a) } A \cup (A \cap B) = A \quad \text{and} \quad \text{(b) } A \cap (A \cup B) = A.$$
11. *Complements of U and $\varnothing$:*
$$\text{(a) } U^c = \varnothing \quad \text{and} \quad \text{(b) } \varnothing^c = U.$$
12. *Set Difference Law:* For all sets A and B,
$$A - B = A \cap B^c.$$

The conclusion of each part of Theorem 6.2.2 is that one set equals another set. As we noted in Section 6.1,

$$\text{Two sets are equal} \iff \text{each is a subset of the other.}$$

The method derived from this fact is the most basic way to prove equality of sets.

Basic Method for Proving That Sets Are Equal

Let sets X and Y be given. To prove that $X = Y$:

1. Prove that $X \subseteq Y$.
2. Prove that $Y \subseteq X$.

Example 6.2.2 **Proof of a Distributive Law**

Consider trying to prove that for all sets A, B, and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Solution The proof of this fact is somewhat more complicated than the proofs in Example 6.2.1, so we first derive its logical structure, then find the core arguments, and end with a formal proof as a summary. As in the subset relation examples, the statement to be proved is universal. Thus, by the method of generalizing from the generic particular, the proof has the following outline:

Starting Point: Suppose A, B, and C are arbitrarily chosen sets.

To Show: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Now two sets are equal if, and only if, each is a subset of the other. Hence, the following two statements must be proved:

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

and

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

Showing the first subset relation requires showing that

$$\forall x, \text{ if } x \in A \cup (B \cap C) \text{ then } x \in (A \cup B) \cap (A \cup C).$$

Showing the second containment requires showing that

$$\forall x, \text{ if } x \in (A \cup B) \cap (A \cup C) \text{ then } x \in A \cup (B \cap C).$$

Note that both of these statements are universal. So to prove the first containment, you

suppose you have any element x in $A \cup (B \cap C)$,

and then you

show that $x \in (A \cup B) \cap (A \cup C)$.

And to prove the second containment, you

suppose you have any element x in $(A \cup B) \cap (A \cup C)$,

and then you

show that $x \in A \cup (B \cap C)$.

In Figure 6.2.1, the structure of the proof is illustrated by the kind of diagram that is often used in connection with structured programs. The analysis in the diagram reduces the proof to two concrete tasks: filling in the steps indicated by dots in the two center boxes of Figure 6.2.1.

Suppose A, B, and C are sets. *[Show $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. That is, show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.]*

Show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. *[That is, show $\forall x$, if $x \in A \cup (B \cap C)$ then $x \in (A \cup B) \cap (A \cup C)$.]*

Suppose $x \in A \cup (B \cap C)$. *[Show $x \in (A \cup B) \cap (A \cup C)$.]*

$\vdots$

Thus $x \in (A \cup B) \cap (A \cup C)$.

Hence $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. *[That is, show $\forall x$, if $x \in (A \cup B) \cap (A \cup C)$ then $x \in A \cup (B \cap C)$.]*

Suppose $x \in (A \cup B) \cap (A \cup C)$. *[Show $x \in A \cup (B \cap C)$.]*

$\vdots$

Thus $x \in A \cup (B \cap C)$.

Hence $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Thus $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$.

FIGURE 6.2.1

The following proof shows the steps for filling in the two innermost boxes of Figure 6.2.1. As you read it, notice how the procedural version of the definition of union is used. For example:

> If you know that $x \in B$, then you can conclude that $x \in A \cup B$ because the statement "$x \in A$ or $x \in B$" is true.

Similarly:

> If you know that $x \in A$, then you can conclude that $x \in A \cup (B \cap C)$ because the statement "$x \in A$ or $x \in B \cap C$" is true.

Also suppose you know that an element—say x—is in a union of two sets but you don't know which set x is in. If you want to deduce a conclusion about x, you need to show that the conclusion follows regardless of which set x is in. So you need to break your argument into two cases: x is in the first set and x is in the second set.

The proof has a few blanks for you to fill in as practice for writing set theory proofs on your own. To make the proof more concise, the symbols $\cap$ and $\cup$ are used in place of the words "intersection" and "union," respectively.

Theorem 6.2.2(3)(a) A Distributive Law for Sets

For all sets A, B, and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Proof: Suppose A, B, and C are any sets.

(1) *Proof that* $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$*:*

Let $x \in A \cup (B \cap C)$. *[We must show that* $x \in$ (a)*.]*

By definition of $\cup$, $x \in$ (b) or $x \in B \cap C$.

Case 1 **($x \in A$)*:*** Since $x \in A$, then both statements $x \in A \cup B$ and $x \in A \cup C$ are true by definition of $\cup$. Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of $\cap$.

Case 2 **($x \in B \cap C$)*:*** Since $x \in B \cap C$, then $x \in B$ and $x \in C$ by definition of $\cap$. Since $x \in B$, then $x \in A \cup B$ by definition of $\cup$. Similarly, since $x \in C$, then $x \in A \cup C$ by definition of $\cup$. Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of $\cap$.

Therefore, in both cases 1 and 2, $x \in (A \cup B)$ (c) $(A \cup C)$.

Because x could be any element in $A \cup (B \cap C)$, this argument shows that every element of $A \cup (B \cap C)$ is in $(A \cup B) \cap (A \cup C)$. Hence,

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

by definition of (d).

(2) *Proof that* $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$*:*

Let $x \in (A \cup B) \cap (A \cup C)$. *[We must show that* $x \in A \cup (B \cap C)$*.]*

We consider the two cases: $x \in A$ and $x \notin A$.*

Case 1 **($x \in A$)*:*** In this case, because x is in A, we can conclude immediately that $x \in A \cup (B \cap C)$ by definition of $\cup$.

(continued on page 398)

*The reason to consider the two cases $x \in A$ and $x \notin A$ is that when $x \in (A \cup B) \cap (A \cup C)$, then, by definition of $\cap$, $x \in (A \cup B)$ and $x \in (A \cup C)$. Now one way for this statement to be true is for x to be in A, but, since that may not be the case, the proof must also consider the possibility that x is not in A.

Case 2 ($x \notin A$): In this case, we know that $x \in (A \cup B) \cap (A \cup C)$. Thus, by definition of (a), $x \in A \cup B$ and $x \in A \cup C$.

Because x is in $A \cup B$, then x is in at least one of A or B, and since x is not in A, then x is in B. Similarly, because x is in $A \cup C$, then x is in at least one of A or C, and since x is not in A, then x is in C.

It follows that $x \in B$ (b) $x \in C$, and, thus, $x \in B \cap C$ by definition of $\cap$.

Since $x \in B \cap C$, then by definition of (c), $x \in A \cup (B \cap C)$.

Therefore, in both cases 1 and 2, $x \in A \cup (B \cap C)$.

Because x could be any element in $(A \cup B) \cap (A \cup C)$, this argument shows that every element of $(A \cup B) \cap (A \cup C)$ is in $A \cup (B \cap C)$. Hence, $(A \cup B) \cap (A \cup C)$ (d) $A \cup (B \cap C)$. Thus, $(A \cup B) \cap (A \cup C)$ (d) $A \cup (B \cap C)$ by definition of subset.

(3) *Conclusion:* Since both subset relations have been proved, it follows, by definition of set equality, that (a).

Solution

(1) a. $(A \cup B) \cap (A \cup C)$ b. A c. $\cap$ d. subset
(2) a. $\cap$ b. and c. $\cup$ d. $\subseteq$
(3) a. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

■

In the study of artificial intelligence, the types of reasoning used previously to derive the proof of the distributive law are called *forward chaining* and *backward chaining*. First what is to be shown is viewed as a goal to be reached starting from a certain initial position: the starting point. Analysis of this goal leads to the realization that if a certain job is accomplished, then the goal will be reached. Call this job subgoal 1: SG_1. (For instance, if the goal is to show that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, then SG_1 would be to show that each set is a subset of the other.) Analysis of SG_1 shows that when yet another job is completed, SG_1 will be reached. Call this job subgoal 2: SG_2. Continuing in this way, a chain of argument leading backward from the goal is constructed.

$$\boxed{\text{starting point}} \qquad \longrightarrow SG_3 \longrightarrow SG_2 \longrightarrow SG_1 \longrightarrow \boxed{\text{goal}}$$

At a certain point, backward chaining becomes difficult, but analysis of the current subgoal suggests it may be reachable by a direct line of argument, or, in other words, by forward chaining, beginning at the starting point. Using the information contained in the starting point, another piece of information, I_1, is deduced; from that another piece of information, I_2, is deduced; and so forth until finally one of the subgoals is reached. This completes the chain and proves the theorem. A completed chain is illustrated below.

$$\boxed{\text{starting point}} \qquad \longrightarrow I_1 \longrightarrow I_2 \longrightarrow I_3 \longrightarrow I_4 \longrightarrow SG_3 \longrightarrow SG_2 \longrightarrow SG_1 \longrightarrow \boxed{\text{goal}}$$

Since set complement is defined in terms of *not*, and since unions and intersections are defined in terms of *or* and *and*, it is not surprising that there are analogues of De Morgan's laws of logic for sets.

Example 6.2.3 **Proof of a De Morgan's Law for Sets**

Prove that for all sets A and B, $(A \cup B)^c = A^c \cap B^c$.

Solution As in previous examples, the statement to be proved is universal, and so the starting point of the proof and the conclusion to be shown are as follows:

Starting Point: Suppose A and B are arbitrarily chosen sets.

To Show: $(A \cup B)^c = A^c \cap B^c$

To do this, you must prove both that $(A \cup B)^c \subseteq A^c \cap B^c$ and that $A^c \cap B^c \subseteq (A \cup B)^c$. To prove the first subset relation means to show that

$$\forall x, \text{ if } x \in (A \cup B)^c \text{ then } x \in A^c \cap B^c.$$

And to prove the second subset relation means to show that

$$\forall x, \text{ if } x \in A^c \cap B^c \text{ then } x \in (A \cup B)^c.$$

Since each of these statements is universal and conditional, for the first subset relation, you

suppose $x \in (A \cup B)^c$,

and then you

show that $x \in A^c \cap B^c$.

And for the second subset relation, you

suppose $x \in A^c \cap B^c$,

and then you

show that $x \in (A \cup B)^c$.

To fill in the steps of these arguments, you use the procedural versions of the definitions of complement, union, and intersection, and at crucial points you use De Morgan's laws of logic.

Theorem 6.2.2(9)(a) A De Morgan's Law for Sets

For all sets A and B, $(A \cup B)^c = A^c \cap B^c$.

Proof: Suppose A and B are sets.

Proof that $(A \cup B)^c \subseteq A^c \cap B^c$***:***

[We must show that $\forall x$*, if* $x \in (A \cup B)^c$ *then* $x \in A^c \cap B^c$*.]*

Suppose $x \in (A \cup B)^c$. *[We must show that* $x \in A^c \cap B^c$*.]* By definition of complement,

$$x \notin A \cup B.$$

Now to say that $x \notin A \cup B$ means that

it is false that (x is in A or x is in B).

By De Morgan's laws of logic, this implies that

x is not in A and x is not in B,

which can be written

$$x \notin A \quad \text{and} \quad x \notin B.$$

(continued on page 400)

Hence $x \in A^c$ and $x \in B^c$ by definition of complement. It follows, by definition of intersection, that $x \in A^c \cap B^c$ *[as was to be shown]*. So $(A \cup B)^c \subseteq A^c \cap B^c$ by definition of subset.

Proof that $\boldsymbol{A^c \cap B^c \subseteq (A \cup B)^c}$***:***
[We must show that $\forall x$*, if* $x \in A^c \cap B^c$ *then* $x \in (A \cup B)^c$*.]*
Suppose $x \in A^c \cap B^c$. *[We must show that* $x \in (A \cup B)^c$*.]* By definition of intersection, $x \in A^c$ and $x \in B^c$, and by definition of complement,

$$x \notin A \quad \text{and} \quad x \notin B.$$

In other words,

$$x \text{ is not in } A \text{ and } x \text{ is not in } B.$$

By De Morgan's laws of logic this implies that

$$\text{it is false that } (x \text{ is in } A \text{ or } x \text{ is in } B),$$

which can be written

$$x \notin A \cup B$$

by definition of union. Hence, by definition of complement, $x \in (A \cup B)^c$ *[as was to be shown]*. It follows that $A^c \cap B^c \subseteq (A \cup B)^c$ by definition of subset.

Conclusion: Since both set containments have been proved, $(A \cup B)^c = A^c \cap B^c$ by definition of set equality.

The set property given in the next theorem says that if one set is a subset of another, then their intersection is the smaller of the two sets and their union is the larger of the two sets.

Theorem 6.2.3 Intersection and Union with a Subset

For any sets A and B, if $A \subseteq B$, then

$$\text{(a) } A \cap B = A \quad \text{and} \quad \text{(b) } A \cup B = B.$$

Proof:
Part (a): Suppose A and B are sets with $A \subseteq B$. To show part (a) we must show both that $A \cap B \subseteq A$ and that $A \subseteq A \cap B$. We already know that $A \cap B \subseteq A$ by the inclusion of intersection property. To show that $A \subseteq A \cap B$, let x be any element in A. *[We must show that* x *is in* $A \cap B$*.]* But, because of the hypothesis that $A \subseteq B$, we can conclude that x is also in B by definition of subset. Hence

$$x \in A \quad \text{and} \quad x \in B,$$

and thus

$$x \in A \cap B$$

by definition of intersection *[as was to be shown]*.

Proof:
Part (b): The proof of part (b) is left as an exercise.

■

The Empty Set

In Section 6.1 we introduced the concept of a set with no elements and promised that in this section we would show that there is only one such set. To do so, we start with the most basic property of a set with no elements: It is a subset of every set. To see why this is true, just ask yourself, "Could it possibly be false? Could there be a set without elements that is *not* a subset of some given set?" The crucial fact is that the negation of a universal statement is existential: If a set B is not a subset of a set A, then there exists an element in B that is not in A. But if B has no elements, then no such element can exist.

Theorem 6.2.4 A Set with No Elements Is a Subset of Every Set

If E is a set with no elements and A is any set, then $E \subseteq A$.

Proof (by contradiction): Suppose not. *[We take the negation of the theorem and suppose it to be true.]* Suppose there exists a set E with no elements and a set A such that $E \not\subseteq A$. *[We must deduce a contradiction.]* Then there would be an element of E that is not an element of A *[by definition of subset]*. But there can be no such element since E has no elements. This is a contradiction. *[Hence the supposition that there are sets E and A, where E has no elements and $E \not\subseteq A$, is false, and so the theorem is true.]*

The truth of Theorem 6.2.4 can also be understood by appeal to the notion of vacuous truth. If E is a set with no elements and A is any set, then to say that $E \subseteq A$ is the same as saying that

$$\forall x, \text{ if } x \in E, \text{ then } x \in A.$$

But since E has no elements, this conditional statement is vacuously true.

How many sets with no elements are there? Only one.

Corollary 6.2.5 Uniqueness of the Empty Set

There is only one set with no elements.

Proof: Suppose E_1 and E_2 are both sets with no elements. By Theorem 6.2.4, $E_1 \subseteq E_2$ since E_1 has no elements. Also $E_2 \subseteq E_1$ since E_2 has no elements. Thus $E_1 = E_2$ by definition of set equality.

It follows from Corollary 6.2.5 that the set of all the pink elephants on earth is equal to the set of all the real numbers whose square is -1 because neither set has any elements! Since there is only one set with no elements, we are justified in calling it by a special name, the empty set (or null set) and in denoting it by the special symbol $\varnothing$.

Note that whereas $\varnothing$ is the set with no elements, the set $\{\varnothing\}$ has one element, the empty set. This is similar to the convention in the computer programming languages Lisp and Scheme, in which ( ) denotes the empty list and (( )) denotes the list whose one element is the empty list.

Suppose you need to show that a certain set equals the empty set. By Corollary 6.2.5 it suffices to show that the set has no elements. For since there is only one set with no elements (namely $\varnothing$), if the given set has no elements, then it must equal $\varnothing$.

Element Method for Proving a Set Equals the Empty Set

To prove that a set X is equal to the empty set $\emptyset$, prove that X has no elements. To do this, suppose X has an element and derive a contradiction.

Example 6.2.4 **Proving That a Set Is Empty**

Prove Theorem 6.2.2(8)(b). That is, prove that for any set A, $A \cap \emptyset = \emptyset$.

Solution Let A be a *[particular, but arbitrarily chosen]* set. To show that $A \cap \emptyset = \emptyset$, it suffices to show that $A \cap \emptyset$ has no elements *[by the element method for proving a set equals the empty set]*. Suppose not. That is, suppose there is at least one element—say x—such that $x \in A \cap \emptyset$. Then, by definition of intersection, $x \in A$ and $x \in \emptyset$. In particular, $x \in \emptyset$. But this is impossible since $\emptyset$ has no elements. *[This contradiction shows that the supposition that there is an element x in $A \cap \emptyset$ is false. So $A \cap \emptyset$ has no elements, as was to be shown.]* Thus $A \cap \emptyset = \emptyset$. ■

Example 6.2.5 **A Proof for a Conditional Statement**

Prove that for all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \emptyset$.

Solution Because the statement to be proved is both universal and conditional, you start with the method of direct proof:

Suppose A, B, and C are arbitrarily chosen sets that satisfy the condition: $A \subseteq B$ and $B \subseteq C^c$.

Show that $A \cap C = \emptyset$.

Since the conclusion to be shown is that a certain set is empty, you can use the principle for proving that a set equals the empty set. A complete proof is shown below.

Proposition 6.2.6

For all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \emptyset$.

Proof: Suppose A, B, and C are any sets such that $A \subseteq B$ and $B \subseteq C^c$. We must show that $A \cap C = \emptyset$. Suppose not. That is, suppose there is an element x in $A \cap C$. By definition of intersection, $x \in A$ and $x \in C$. Then, since $A \subseteq B$, $x \in B$ by definition of subset. Also, since $B \subseteq C^c$, then $x \in C^c$ by definition of subset again. It follows by definition of complement that $x \notin C$. Thus $x \in C$ and $x \notin C$, which is a contradiction. So the supposition that there is an element x in $A \cap C$ is false, and thus $A \cap C = \emptyset$ *[as was to be shown]*.

■

Example 6.2.6 **A Generalized Distributive Law**

Prove that for all sets A and $B_1, B_2, B_3, \ldots, B_n$, where n is a positive integer,

$$A \cup \left(\bigcap_{i=1}^{n} B_i \right) = \bigcap_{i=1}^{n} (A \cup B_i).$$

Solution Compare this proof to the one given in Example 6.2.2. Although the notation is more complex, the basic ideas are the same.

Proof: Suppose A and $B_1, B_2, B_3, \ldots, B_n$ are any sets and n is a positive integer.

Part 1, Proof that $\boldsymbol{A \cup \left(\bigcap_{i=1}^{n} B_i\right) \subseteq \bigcap_{i=1}^{n} (A \cup B_i)}$***:***

Suppose x is any element in $A \cup \left(\bigcap_{i=1}^{n} B_i\right)$. *[We must show that x is in $\bigcap_{i=1}^{n} (A \cup B_i)$.]*

By definition of union, $x \in A$ or $x \in \bigcap_{i=1}^{n} B_i$.

Case 1, $\boldsymbol{x \in A}$***:*** In this case, it is true by definition of union that for every integer $i = 1, 2, \ldots, n$, $x \in A \cup B_i$. Hence $x \in \bigcap_{i=1}^{n} (A \cup B_i)$.

Case 2, $\boldsymbol{x \in \bigcap_{i=1}^{n} B_i}$***:*** In this case, by definition of the general intersection, we have that for every integer $i = 1, 2, \ldots, n$, $x \in B_i$. Hence, by definition of union, for every integer $i = 1, 2, \ldots, n$, $x \in A \cup B_i$, and so, by definition of general intersection, $x \in \bigcap_{i=1}^{n} (A \cup B_i)$.

Thus, in either case, $x \in \bigcap_{i=1}^{n} (A \cup B_i)$ *[as was to be shown].*

Part 2, Proof that $\boldsymbol{\bigcap_{i=1}^{n} (A \cup B_i) \subseteq A \cup \left(\bigcap_{i=1}^{n} B_i\right)}$***:***

Suppose x is any element in $\bigcap_{i=1}^{n} (A \cup B_i)$ *[We must show that x is in $A \cup \bigcap_{i=1}^{n} B_i$.]*

By definition of intersection, $x \in A \cup B_i$ for every integer $i = 1, 2, \ldots, n$. Either $x \in A$ or $x \notin A$.

Case 1, $\boldsymbol{x \in A}$***:*** In this case, $x \in A \cup \left(\bigcap_{i=1}^{n} B_i\right)$ by definition of union.

Case 2, $\boldsymbol{x \notin A}$***:*** By definition of intersection, $x \in A \cup B_i$ for every integer $i = 1, 2, \ldots, n$. Since $x \notin A$, x must be in each B_i for every integer $i = 1, 2, \ldots, n$. Hence, by definition of intersection, $x \in \bigcap_{i=1}^{n} B_i$, and so, by definition of union, $x \in A \cup \left(\bigcap_{i=1}^{n} B_i\right)$.

Conclusion: Since both set containments have been proved, it follows by definition of set equality that $A \cup \left(\bigcap_{i=1}^{n} B_i\right) = \bigcap_{i=1}^{n} (A \cup B_i)$. ■

TEST YOURSELF

1. To prove that a set X is a subset of a set $A \cap B$, you suppose that x is any element of X and you show that $x \in A$ _____ $x \in B$.
2. To prove that a set X is a subset of a set $A \cup B$, you suppose that x is any element of X and you show that $x \in A$ _____ $x \in B$.
3. To prove that a set $A \cup B$ is a subset of a set X, you start with any element x in $A \cup B$ and consider the two cases _____ and _____. You then show that in either case _____.
4. To prove that a set $A \cap B$ is a subset of a set X, you suppose that _____ and you show that_____.

5. To prove that a set X equals a set Y, you prove that _____ and that_____.

6. To prove that a set X does not equal a set Y, you need to find an element that is in _____ and not _____ or that is in _____ and not _____.

EXERCISE SET 6.2

1. a. To say that an element is in $A \cap (B \cup C)$ means that it is in $\underline{\quad(1)\quad}$ and in $\underline{\quad(2)\quad}$.

b. To say that an element is in $(A \cap B) \cup C$ means that it is in $\underline{\quad(1)\quad}$ or in $\underline{\quad(2)\quad}$.

c. To say that an element is in $A - (B \cap C)$ means that it is in $\underline{\quad(1)\quad}$ and not in $\underline{\quad(2)\quad}$.

d. To prove that $(A \cup B) \cap C \subseteq A \cup (B \cap C)$, we suppose that x is any element in $\underline{\quad(1)\quad}$. Then we must show that $\underline{\quad(2)\quad}$.

e. If A, B, and C are any sets such that $B \subseteq C$, to prove that $A \cap B \subseteq A \cap C$, we suppose that x is any element in $\underline{\quad(1)\quad}$. Then we must show that $\underline{\quad(2)\quad}$.

2. The following are two proofs that for all sets A and B, $A - B \subseteq A$. The first is less formal, and the second is more formal. Fill in the blanks.

a. Proof: Suppose A and B are any sets. To show that $A - B \subseteq A$, we must show that every element in $\underline{\quad(1)\quad}$ is in $\underline{\quad(2)\quad}$. But any element in $A - B$ is in $\underline{\quad(3)\quad}$ and not in $\underline{\quad(4)\quad}$ (by definition of $A - B$). In particular, such an element is in A.

b. Proof: Suppose A and B are any sets and $x \in A - B$. *[We must show that* $\underline{\quad(1)\quad}$*.]* By definition of set difference, $x \in$ $\underline{\quad(2)\quad}$ and $x \notin$ $\underline{\quad(3)\quad}$. In particular, $x \in$ $\underline{\quad(4)\quad}$ *[which is what was to be shown].*

In 3 and 4, supply explanations of the steps in the given proofs.

3. Theorem: For all sets A, B, and C, if $A \subseteq B$, $B \subseteq C$, then $A \subseteq C$.

Proof:

Statement	Explanation
Suppose A, B, and C are any sets such that $A \subseteq B$ and $B \subseteq C$.	starting point
We must show that $A \subseteq C$.	conclusion to be shown
Let x be any element in A.	start of an element proof
Then x is in B.	$\underline{\quad(a)\quad}$
It follows that x is in C.	$\underline{\quad(b)\quad}$
Thus every element in A is in C.	since x could be any element of A
Therefore, $A \subseteq C$ *[as was to be shown].*	$\underline{\quad(c)\quad}$

4. Theorem: For all sets A and B, if $A \subseteq B$, then $A \cup B \subseteq B$.

Proof:

Statement	Explanation
Suppose A, B, and C are any sets such that $A \subseteq B$.	starting point
We must show that $A \cup B \subseteq B$.	conclusion to be shown
Let x be any element in $A \cup B$.	start of an element proof
Then x is in A or x is in B.	$\underline{\quad(a)\quad}$
In case x is in A, then x is in B.	$\underline{\quad(b)\quad}$
In case x is in B, then x is in B.	tautology ($p \rightarrow p$)
So in either case x is in B.	proof by division into cases
Thus every element in $A \cup B$ is in B.	since x could be any element of $A \cup B$
Therefore, $A \cup B \subseteq B$ *[as was to be shown].*	$\underline{\quad(c)\quad}$

5. Prove that for all sets A and B, $(B - A) = B \cap A^c$.

***H* 6.** Let $\cap$ and $\cup$ stand for the words "intersection" and "union," respectively. Fill in the blanks in the following proof that for all sets A, B, and C, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof: Suppose A, B, and C are any sets.

(1) *Proof that* $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$**:** Let $x \in A \cap (B \cup C)$. *[We must show that* $x \in$ (a)*].*

By definition of $\cap$, $x \in$ (b) and $x \in B \cup C$.

Thus $x \in A$ and, by definition of $\cup$, $x \in B$ or (c) .

Case 1 $(x \in A$ **and** $x \in B)$**:** In this case, $x \in A \cap B$ by definition of $\cap$.

Case 2 $(x \in A$ **and** $x \in C)$**:** In this case, $x \in A \cap C$ by definition of $\cap$.

By cases 1 and 2, $x \in A \cap B$ or $x \in A \cap C$, and so, by definition of $\cup$, (d).

[So $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ *by definition of subset.]*

(2) *Proof that* $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$**:** Let $x \in (A \cap B) \cup (A \cap C)$. *[We must show that* $x \in A \cap (B \cup C)$*.]*

By definition of $\cup$, $x \in A \cap B$ (a) $x \in A \cap C$.

Case 1 $(x \in A \cap B)$**:** In this case, by definition of $\cap$, $x \in A$ and $x \in B$.

Since $x \in B$, then $x \in B \cup C$ by definition of $\cup$.

Case 2 $(x \in A \cap C)$**:** In this case, by definition of $\cap$, $x \in A$ (b) $x \in C$.

Since $x \in C$, then $x \in B \cup C$ by definition of $\cup$.

In both cases $x \in A$ and $x \in B \cup C$, and so, by definition of $\cap$, (c).

[So $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ by definition of (d)*.]*

(3) *Conclusion:* *[Since both subset relations have been proved, it follows, by definition of set equality, that* (a)*.]*

Use an element argument to prove each statement in 7–22. Assume that all sets are subsets of a universal set U.

H 7. For all sets A and B, $(A \cap B)^c = A^c \cup B^c$.

8. For all sets A and B, $(A \cap B) \cup (A \cap B^c) = A$. (This property is used in Section 9.9.)

H 9. For all sets A, B, and C,
$$(A - B) \cup (C - B) = (A \cup C) - B.$$

10. For all sets A, B, and C, $(A \cup B) \cap C \subseteq A \cup (B \cap C)$.

11. For all sets A, B, and C, $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$.

12. For all sets A, B, and C, $(A \cup B) - C \subseteq (A - C) \cup (B - C)$.

13. For all sets A, B, and C,
$$(A - B) \cap (C - B) = (A \cap C) - B.$$

H 14. For all sets A and B, $A \cup (A \cap B) = A$.

15. For every set A, $A \cup \varnothing = A$.

16. For all sets A, B, and C, if $A \subseteq B$ then $A \cap C \subseteq B \cap C$.

17. For all sets A, B, and C, if $A \subseteq B$ then $A \cup C \subseteq B \cup C$.

18. For all sets A and B, if $A \subseteq B$ then $B^c \subseteq A^c$.

H 19. For all sets A, B, and C, if $A \subseteq B$ and $A \subseteq C$ then $A \subseteq B \cap C$.

20. For all sets A, B, and C, if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

21. For all sets A, B, and C,
$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

22. For all sets A, B, and C,
$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

23. Find the mistake in the following "proof" that for all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

"**Proof:** Suppose A, B, and C are any sets such that $A \subseteq B$ and $B \subseteq C$. Since $A \subseteq B$, there is an element x such that $x \in A$ and $x \in B$, and since $B \subseteq C$, there is an element x such that $x \in B$ and $x \in C$. Hence there is an element x such that $x \in A$ and $x \in C$ and so $A \subseteq C$."

H 24. Find the mistake in the following "proof."

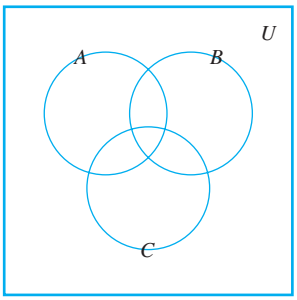
"Theorem:" For all sets A and B, $A^c \cup B^c \subseteq (A \cup B)^c$.

"**Proof:** Suppose A and B are any sets, and $x \in A^c \cup B^c$. Then $x \in A^c$ or $x \in B^c$ by definition of union. It follows that $x \notin A$ or $x \notin B$ by definition of complement, and so $x \notin A \cup B$ by definition of union. Thus $x \in (A \cup B)^c$ by definition of complement, and hence $A^c \cup B^c \subseteq (A \cup B)^c$."

25. Find the mistake in the following "proof" that for all sets A and B, $(A - B) \cup (A \cap B) \subseteq A$.

"**Proof:** Suppose A and B are any sets, and suppose $x \in (A - B) \cup (A \cap B)$. If $x \in A$ then $x \in A - B$, and so, by definition of difference, $x \in A$ and $x \notin B$. In particular, $x \in A$, and, therefore, $(A - B) \cup (A \cap B) \subseteq A$ by definition of subset."

26. Consider the Venn diagram below.



a. Illustrate one of the distributive laws by shading in the region corresponding to $A \cup (B \cap C)$ on one copy of the diagram and $(A \cup B) \cap (A \cup C)$ on another.

b. Illustrate the other distributive law by shading in the region corresponding to $A \cap (B \cup C)$ on one copy of the diagram and $(A \cap B) \cup (A \cap C)$ on another.

c. Illustrate one of De Morgan's laws by shading in the region corresponding to $(A \cup B)^c$ on one copy of the diagram and $A^c \cap B^c$ on the other. (Leave the set C out of your diagrams.)

d. Illustrate the other De Morgan's law by shading in the region corresponding to $(A \cap B)^c$ on one copy of the diagram and $A^c \cup B^c$ on the other. (Leave the set C out of your diagrams.)

27. Fill in the blanks in the following proof that for all sets A and B, $(A - B) \cap (B - A) = \varnothing$.

Proof: Let A and B be any sets and suppose $(A - B) \cap (B - A) \neq \varnothing$. That is, suppose there is an element x in _____(a)_____. By definition of _____(b)_____, $x \in A - B$ and $x \in$ _____(c)_____. Then by definition of set difference, $x \in A$ and $x \notin B$ and $x \in$ _____(d)_____ and $x \notin$ _____(e)_____. In particular $x \in A$ and $x \notin$ _____(f)_____, which is a contradiction. Hence *[the supposition that* $(A - B) \cap (B - A) \neq \varnothing$ *is false, and so]* _____(g)_____.

Use the element method for proving a set equals the empty set to prove each statement in 28–38. Assume that all sets are subsets of a universal set U.

28. For all sets A and B, $(A \cap B) \cap (A \cap B^c) = \varnothing$. (This property is used in Section 9.9.)

29. For all sets A, B, and C,

$$(A - C) \cap (B - C) \cap (A - B) = \varnothing.$$

30. For every subset A of a universal set U, $A \cap A^c = \varnothing$.

31. If U denotes a universal set, then $U^c = \varnothing$.

32. For every set A, $A \times \varnothing = \varnothing$.

33. For all sets A and B, if $A \subseteq B$ then $A \cap B^c = \varnothing$.

34. For all sets A and B, if $B \subseteq A^c$ then $A \cap B = \varnothing$.

35. For all sets A, B, and C, if $A \subseteq B$ and $B \cap C = \varnothing$ then $A \cap C = \varnothing$.

36. For all sets A, B, and C, if $C \subseteq B - A$, then $A \cap C = \varnothing$.

37. For all sets A, B, and C,

if $B \cap C \subseteq A$, then $(C - A) \cap (B - A) = \varnothing$.

38. For all sets A, B, C, and D,

if $A \cap C = \varnothing$ then $(A \times B) \cap (C \times D) = \varnothing$.

Prove each statement in 39–44.

H **39.** For all sets A and B,

a. $(A - B) \cup (B - A) \cup (A \cap B) = A \cup B$

b. The sets $(A - B)$, $(B - A)$, and $(A \cap B)$ are mutually disjoint.

40. For every positive integer n, if A and $B_1, B_2, B_3, \ldots$ are any sets, then

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \cap B_i).$$

H **41.** For every positive integer n, if $A_1, A_2, A_3, \ldots$ and B are any sets, then

$$\bigcup_{i=1}^{n} (A_i - B) = \left(\bigcup_{i=1}^{n} A_i \right) - B.$$

42. For every positive integer n, if $A_1, A_2, A_3, \ldots$ and B are any sets, then

$$\bigcap_{i=1}^{n} (A_i - B) = \left(\bigcap_{i=1}^{n} A_i \right) - B.$$

43. For every positive integer n, if A and $B_1, B_2, B_3, \ldots$ are any sets, then

$$\bigcup_{i=1}^{n}(A \times B_i) = A \times \left(\bigcup_{i=1}^{n} B_i\right).$$

44. For every positive integer n, if A and $B_1, B_2, B_3, \ldots$ are any sets, then

$$\bigcap_{i=1}^{n}(A \times B_i) = A \times \left(\bigcap_{i=1}^{n} B_i\right).$$

ANSWERS FOR TEST YOURSELF

1. and **2.** or **3.** $x \in A$; $x \in B$; $x \in X$ **4.** $x \in A \cap B$ (*Or:* x is an element of both A and B); $x \in X$ **5.** $X \subseteq Y$; $Y \subseteq X$ **6.** X; in Y; Y; in X

6.3 Disproofs and Algebraic Proofs

If a fact goes against common sense, and we are nevertheless compelled to accept and deal with this fact, we learn to alter our notion of common sense.
—Phillip J. Davis and Reuben Hersh, *The Mathematical Experience*, 1981

In Section 6.2 we gave examples only of set properties that were true. Occasionally, however, a proposed set property is false. We begin this section by discussing how to disprove such a proposed property. Then we prove an important theorem about the power set of a set and go on to discuss an "algebraic" method for deriving new set properties from set properties already known to be true. We finish the section with an introduction to Boolean algebras.

Disproving an Alleged Set Property

Recall that to show a universal statement is false, it suffices to find one example (called a counterexample) for which it is false.

Example 6.3.1 **Finding a Counterexample for a Set Identity**

Is the following set property true?

For all sets A, B, and C, $(A - B) \cup (B - C) = A - C$.

Solution Observe that the property is true if, and only if,

the given equality holds for *all* sets A, B, and C.

So it is false if, and only if,

there are sets A, B, and C for which the equality does *not* hold.

One way to solve this problem is to picture sets A, B, and C by drawing a Venn diagram such as that shown in Figure 6.3.1 on the next page. If you assume that any of the eight regions of the diagram may be empty of points, then the diagram is quite general.

Find and shade the region corresponding to $(A - B) \cup (B - C)$. Then shade the region corresponding to $A - C$. These are shown in Figure 6.3.2 on the next page.

Comparing the shaded regions seems to indicate that the property is false. For instance, if there is an element in B that is not in either A or C then this element would be in $(A - B) \cup (B - C)$ (because of being in B and not C), but it would not be in $A - C$ since $A - C$ contains nothing outside A. Similarly, an element that is in both A and C but not B

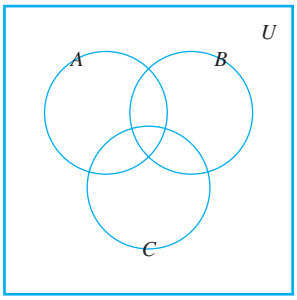
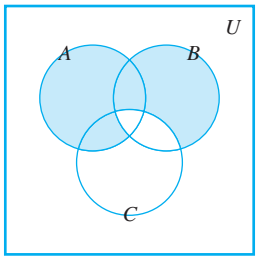


FIGURE 6.3.1

would be in $(A - B) \cup (B - C)$ (because of being in A and not B), but it would not be in $A - C$ (because of being in both A and C).



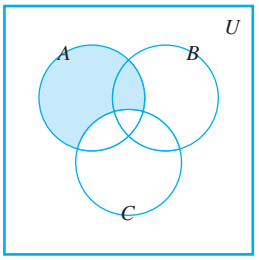


FIGURE 6.3.2

Construct a concrete counterexample in order to confirm your answer and make sure that you did not make a mistake either in drawing or analyzing your diagrams. One way is to put one of the integers from 1 through 7 into each of the seven subregions enclosed by the circles representing A, B, and C. If the proposed set property had involved set complements, it would also be helpful to label the region outside the circles, and so we place the number 8 there. (See Figure 6.3.3.) Then define discrete sets A, B, and C to consist of all the numbers in their respective subregions.

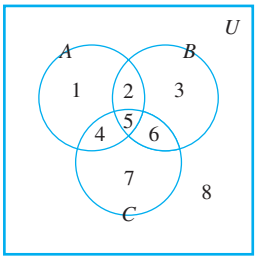


FIGURE 6.3.3

Counterexample 1: Let $A = \{1, 2, 4, 5\}$, $B = \{2, 3, 5, 6\}$, and $C = \{4, 5, 6, 7\}$. Then

$$A - B = \{1, 4\}, \quad B - C = \{2, 3\}, \quad \text{and} \quad A - C = \{1, 2\}.$$

Hence

$$(A - B) \cup (B - C) = \{1, 4\} \cup \{2, 3\} = \{1, 2, 3, 4\}, \quad \text{whereas} \quad A - C = \{1, 2\}.$$

Since $\{1, 2, 3, 4\} \neq \{1, 2\}$, we have that $(A - B) \cup (B - C) \neq A - C$.

A more economical counterexample can be obtained by observing that as long as the set B contains an element, such as 3, that is not in A, then regardless of whether B contains any other elements and regardless of whether A and C contain any elements at all, $(A - B) \cup (B - C) \neq A - C$.

Counterexample 2: Let $A = \emptyset$, $B = \{3\}$, and $C = \emptyset$. Then

$$A - B = \emptyset, \quad B - C = \{3\}, \quad \text{and} \quad A - C = \emptyset.$$

Hence $(A - B) \cup (B - C) = \emptyset \cup \{3\} = \{3\}$, whereas $A - C = \emptyset$.

Since $\{3\} \neq \emptyset$, we have that $(A - B) \cup (B - C) \neq A - C$.

Note Check that when $A = C = \{4\}$ and $B = \emptyset$, $(A - B) \cup (B - C) \neq A - C$.

Another economical counterexample requires only that $A = C =$ a singleton set, such as $\{4\}$, while B is the empty set. ■

Problem-Solving Strategy

How can you discover whether a given universal statement about sets is true or false? There are two basic approaches. Either you plunge in and start trying to prove the statement, asking yourself, "What do I need to show?" and "How do I show it?" or you try to find a set of conditions that must be fulfilled to construct a counterexample. With either approach you may have immediate success or you may run into difficulty. The trick is to be ready to switch to the other approach if the one you are working on does not look promising. For more difficult questions, you may alternate several times between the two approaches before arriving at the correct answer.

The Number of Subsets of a Set

The following theorem states the important fact that if a set has n elements then its power set has 2^n elements. The proof uses mathematical induction and is based on the following observations. Suppose X is a set and z is an element of X.

1. The subsets of X can be split into two groups: those that do not contain z and those that do contain z.
2. The subsets of X that do not contain z are the same as the subsets of $X - \{z\}$.
3. The subsets of X that do not contain z can be matched up one for one with the subsets of X that do contain z by matching each subset A that does not contain z to the subset $A \cup \{z\}$ that contains z. Thus there are as many subsets of X that contain z as there are subsets of X that do not contain z. For instance, if $X = \{x, y, z\}$, the following table shows the correspondence between subsets of X that do not contain z and subsets of X that contain z.

Subsets of X That Do Not Contain z		Subsets of X That Contain z
$\emptyset$	$\leftrightarrow$	$\emptyset \cup \{z\} = \{z\}$
$\{x\}$	$\leftrightarrow$	$\{x\} \cup \{z\} = \{x, z\}$
$\{y\}$	$\leftrightarrow$	$\{y\} \cup \{z\} = \{y, z\}$
$\{x, y\}$	$\leftrightarrow$	$\{x, y\} \cup \{z\} = \{x, y, z\}$

Theorem 6.3.1

For every integer $n \geq 0$, if a set X has n elements, then $\mathcal{P}(X)$ has 2^n elements.

Proof (by mathematical induction): Let the property $P(n)$ be the sentence

Any set with n elements has 2^n subsets. ← $P(n)$

Show that P(0) is true:
To establish $P(0)$, we must show that

Any set with 0 elements has 2^0 subsets. ← $P(0)$

Now the only set with zero elements is the empty set, and the only subset of the empty set is itself. Thus a set with zero elements has one subset. Since $1 = 2^0$, we have that $P(0)$ is true.

Show that for every integer $k \geq 0$, if $P(k)$ is true then $P(k+1)$ is also true:
[Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 0$. That is:]
Suppose that k is any integer with $k \geq 0$ such that

Any set with k elements has 2^k subsets. ← $P(k)$ inductive hypothesis

[We must show that $P(k+1)$ is true. That is:] We must show that

Any set with $k+1$ elements has 2^{k+1} subsets. ← $P(k+1)$

Let X be a set with $k+1$ elements. Since $k+1 \geq 1$, we may pick an element z in X. Observe that any subset of X either contains z or does not. Furthermore, any subset of X that does not contain z is a subset of $X - \{z\}$. And any subset A of $X - \{z\}$ can be matched up with a subset B, equal to $A \cup \{z\}$, of X that contains z. Consequently, there are as many subsets of X that contain z as do not, and thus there are twice as many subsets of X as there are subsets of $X - \{z\}$. It follows that since $X - \{z\}$ has k elements, then, by inductive hypothesis,

$$\text{the number of subsets of } X - \{z\} = 2^k$$

Therefore,

$$\begin{aligned} \text{the number of subsets of } X &= 2 \cdot (\text{the number of subsets of } X - \{z\}) \\ &= 2 \cdot (2^k) && \text{by substitution} \\ &= 2^{k+1} && \text{by basic algebra.} \end{aligned}$$

[This is what was to be shown.]
[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

"Algebraic" Proofs of Set Identities

Let U be a universal set and consider the power set of U, $\mathcal{P}(U)$. The set identities given in Theorem 6.2.2 hold for all elements of $\mathcal{P}(U)$. Once a certain number of identities and other properties have been established, new properties can be derived from them algebraically without having to use element method arguments. It turns out that only identities (1–5) of Theorem 6.2.2 are needed to prove any other identity involving only unions, intersections, and complements. With the addition of identity (12), the set difference law,

any set identity involving unions, intersections, complements, and set differences can be established.

To use known properties to derive new ones, you need to use the fact that such properties are universal statements. Like the laws of algebra for real numbers, they apply to a wide variety of different situations. Assume that all sets are subsets of $\mathcal{P}(U)$, then, for instance, one of the distributive laws states that

$$\text{for all sets } A, B, \text{ and } C, \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

This law can be viewed as a general template into which *any* three particular sets can be placed. Thus, for example, if A_1, A_2, and A_3 represent particular sets, then

$$\underbrace{A_1} \cap (\underbrace{A_2} \cup \underbrace{A_3}) = (\underbrace{A_1} \cap \underbrace{A_2}) \cup (\underbrace{A_1} \cap \underbrace{A_3}),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

where A_1 takes the place of A, A_2 takes the place of B, and A_3 takes the place of C. Similarly, if W, X, Y, and Z are any particular sets, then, by the distributive law,

$$\underbrace{(W \cap X)} \cap (Y \cup Z) = ((\underbrace{W \cap X}) \cap Y) \cup ((\underbrace{W \cap X}) \cap Z),$$
$$\updownarrow \quad \updownarrow \quad \updownarrow \qquad \updownarrow \quad \updownarrow \qquad \updownarrow \quad \updownarrow$$
$$A \quad \cap (B \cup C) = \quad (A \quad \cap B) \cup \quad (A \quad \cap C)$$

where $W \cap X$ takes the place of A, Y takes the place of B, and Z takes the place of C.

Example 6.3.2 **Deriving a Set Difference Property**

Construct an algebraic proof that for all sets A, B, and C,

$$(A \cup B) - C = (A - C) \cup (B - C).$$

Cite a property from Theorem 6.2.2 for each step of the proof.

Solution Let A, B, and C be any sets. Then

$$\begin{aligned}
(A \cup B) - C &= (A \cup B) \cap C^c && \text{by the set difference law} \\
&= C^c \cap (A \cup B) && \text{by the commutative law for } \cap \\
&= (C^c \cap A) \cup (C^c \cap B) && \text{by the distributive law} \\
&= (A \cap C^c) \cup (B \cap C^c) && \text{by the commutative law for } \cap \\
&= (A - C) \cup (B - C) && \text{by the set difference law.}
\end{aligned}$$

■

Example 6.3.3 **Deriving a Set Identity Using Properties of $\varnothing$**

Construct an algebraic proof that for all sets A and B,

$$A - (A \cap B) = A - B.$$

Cite a property from Theorem 6.2.2 for every step of the proof.

Solution Suppose A and B are any sets. Then

$$\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c && \text{by the set difference law} \\
&= A \cap (A^c \cup B^c) && \text{by De Morgan's law} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{by the distributive law} \\
&= \varnothing \cup (A \cap B^c) && \text{by the complement law} \\
&= (A \cap B^c) \cup \varnothing && \text{by the commutative law for } \cup \\
&= A \cap B^c && \text{by the identity law for } \cup \\
&= A - B && \text{by the set difference law.}
\end{aligned}$$

■

To many people an algebraic proof seems simpler than an element proof, but often an element proof is actually easier to understand. For instance, in Example 6.3.3 above, you could see immediately that $A - (A \cap B) = A - B$ because for an element to be in $A - (A \cap B)$ means that it is in A and not in both A and B, and this is equivalent to saying that it is in A and not in B.

Example 6.3.4 **Deriving a Generalized Associative Law**

Prove that for any sets A_1, A_2, A_3, and A_4,

$$((A_1 \cup A_2) \cup A_3) \cup A_4 = A_1 \cup ((A_2 \cup A_3) \cup A_4).$$

Cite a property from Theorem 6.2.2 for every step of the proof.

Caution! When doing problems similar to Examples 6.3.2–6.3.4, be sure to use the set properties exactly as they are stated in Theorem 6.2.2.

Solution Let A_1, A_2, A_3, and A_4 be any sets. Then

$$((A_1 \cup A_2) \cup A_3) \cup A_4 = (A_1 \cup (A_2 \cup A_3)) \cup A_4$$ by the associative law for $\cup$ with A_1 taking the place of A, A_2 taking the place of B, and A_3 taking the place of C

$$= A_1 \cup ((A_2 \cup A_3) \cup A_4)$$ by the associative law for $\cup$ with A_1 taking the place of A, $A_2 \cup A_3$ taking the place of B, and A_4 taking the place of C.

■

TEST YOURSELF

1. Given a proposed set identity involving set variables A, B, and C, the most common way to show that the equation does not hold in general is to find concrete sets A, B, and C that, when substituted for the set variables in the equation, _____.
2. When using the algebraic method for proving a set identity, it is important to _____ for every step.
3. When applying a property from Theorem 6.2.2, it must be used _____ as it is stated.

EXERCISE SET 6.3

For each of 1–4 find a counterexample to show that the statement is false. Assume all sets are subsets of a universal set U.

1. For all sets A, B, and C,
$$(A \cup B) \cap C = A \cup (B \cap C).$$
2. For all sets A and B, $(A \cup B)^c = A^c \cup B^c$.
3. For all sets A, B, and C, if $A \not\subseteq B$ and $B \not\subseteq C$ then $A \not\subseteq C$.
4. For all sets A, B, and C, if $B \cup C \subseteq A$ then
$$(A - B) \cap (A - C) = \varnothing.$$

For each of 5–21 prove each statement that is true and find a counterexample for each statement that is false. Assume all sets are subsets of a universal set U.

5. For all sets A, B, and C,
$$A - (B - C) = (A - B) - C.$$
6. For all sets A and B, $A \cap (A \cup B) = A$.
7. For all sets A, B, and C,
$$(A - B) \cap (C - B) = A - (B \cup C).$$
8. For all sets A and B, if $A^c \subseteq B$ then $A \cup B = U$.
9. For all sets A, B, and C, if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.
10. For all sets A and B, if $A \subseteq B$ then $A \cap B^c = \varnothing$.

H 11. For all sets A, B, and C, if $A \subseteq B$ then $A \cap (B \cap C)^c = \varnothing$.

H 12. For all sets A, B, and C,
$$A \cap (B - C) = (A \cap B) - (A \cap C).$$

13. For all sets A, B, and C,
$$A \cup (B - C) = (A \cup B) - (A \cup C).$$

H 14. For all sets A, B, and C, if $A \cap C = B \cap C$ and $A \cup C = B \cup C$, then $A = B$.

H 15. For all sets A, B, and C, $(A - B) \cup C \subseteq A \cup (C - B)$.

16. For all sets A and B, if $A \cap B = \emptyset$ then $A \times B = \emptyset$.

17. For all sets A and B, if $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

18. For all sets A and B, $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.

H 19. For all sets A and B, $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

20. For all sets A and B, $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

21. For all sets A and B, $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$.

22. Write a negation for each of the following statements. Indicate which is true, the statement or its negation. Justify your answers.

a. $\forall$ sets S, $\exists$ a set T such that $S \cap T = \emptyset$.

b. $\exists$ a set S such that $\forall$ sets T, $S \cup T = \emptyset$.

H 23. Let $S = \{a, b, c\}$, and for each integer $i = 0, 1, 2, 3$, let S_i be the set of all subsets of S that have i elements. List the elements in S_0, S_1, S_2, and S_3. Is $\{S_0, S_1, S_2, S_3\}$ a partition of $\mathcal{P}$(S)?

24. Let $A = \{t, u, v, w\}$, and let S_1 be the set of all subsets of A that do not contain w and S_2 the set of all subsets of A that contain w.

a. Find S_1.

b. Find S_2.

c. Are S_1 and S_2 disjoint?

d. Compare the sizes of S_1 and S_2.

e. How many elements are in $S_1 \cup S_2$?

f. What is the relation between $S_1 \cup S_2$ and $\mathcal{P}(A)$?

H 25. Use mathematical induction to prove that for every integer $n \geq 2$, if a set S has n elements, then the number of subsets of S with an even number of elements equals the number of subsets of S with an odd number of elements.

H* 26. The following problem, devised by Ginger Bolton, appeared in the January 1989 issue of the *College Mathematics Journal* (Vol. 20, No. 1, p. 68): Given a positive integer $n \geq 2$, let S be the set of all nonempty subsets of $\{2, 3, \ldots, n\}$. For each $S_i \in S$, let P_i be the product of the elements of S_i. Prove or disprove that

$$\sum_{i=1}^{2^{n-1}-1} P_i = \frac{(n+1)!}{2} - 1.$$

In 27 and 28 supply a reason for each step in the derivation.

27. For all sets A, B, and C,

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Proof: Suppose A, B, and C are any sets. Then

$$\begin{aligned}(A \cup B) \cap C &= C \cap (A \cup B) && \text{by (a)}\\ &= (C \cap A) \cup (C \cap B) && \text{by (b)}\\ &= (A \cap C) \cup (B \cap C) && \text{by (c).}\end{aligned}$$

H 28. For all sets A, B, and C,

$$(A \cup B) - (C - A) = A \cup (B - C).$$

Proof: Suppose A, B, and C are any sets. Then

$$\begin{aligned}(A \cup B) - (C - A) &= (A \cup B) \cap (C - A)^c && \text{by (a)}\\ &= (A \cup B) \cap (C \cap A^c)^c && \text{by (b)}\\ &= (A \cup B) \cap (A^c \cap C)^c && \text{by (c)}\\ &= (A \cup B) \cap ((A^c)^c \cup C^c) && \text{by (d)}\\ &= (A \cup B) \cap (A \cup C^c) && \text{by (e)}\\ &= A \cup (B \cap C^c) && \text{by (f)}\\ &= A \cup (B - C) && \text{by (g).}\end{aligned}$$

H 29. Some steps are missing from the following proof that for all sets A and B, $(A \cup B^c) - B = (A - B) \cup B^c$. Indicate what they are, and then write the proof correctly.

Proof: Let any sets A and B be given . Then

$$\begin{aligned}(A \cup B^c) - B &= (A \cup B^c) \cap B^c && \text{by the set difference law}\\ &= (B^c \cap A) \cup (B^c \cap B^c) && \text{by the distributive law}\\ &= (B^c \cap A) \cup B^c && \text{by the idempotent law for } \cup\\ &= (A - B) \cup B^c && \text{by the set difference law.}\end{aligned}$$

In 30–40, construct an algebraic proof for the given statement. Cite a property from Theorem 6.2.2 for every step.

30. For all sets A, B, and C,

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

31. For all sets A and B, $A \cup (B - A) = A \cup B$.

32. For all sets A and B, $(A - B) \cup (A \cap B) = A$.

33. For all sets A and B, $(A - B) \cap (A \cap B) = \emptyset$.

34. For all sets A, B, and C,

$$(A - B) - C = A - (B \cup C).$$

35. For all sets A and B, $A - (A - B) = A \cap B$.

36. For all sets A and B, $((A^c \cup B^c) - A)^c = A$.

37. For all sets A and B, $(B^c \cup (B^c - A))^c = B$.

38. For all sets A and B, $(A \cap B)^c \cap A = A - B$.

39. For all sets A and B,

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B).$$

40. For all sets A, B, and C,

$$(A - B) - (B - C) = A - B.$$

In 41–43 simplify the given expression. Cite a property from Theorem 6.2.2 for every step.

H **41.** $A \cap ((B \cup A^c) \cap B^c)$

42. $(A - (A \cap B)) \cap (B - (A \cap B))$

43. $((A \cap (B \cup C)) \cap (A - B)) \cap (B \cup C^c)$

44. Consider the following set property: For all sets A and B, $A - B$ and B are disjoint.
- **a.** Use an element argument to derive the property.
- **b.** Use an algebraic argument to derive the property (by applying properties from Theorem 6.2.2).
- **c.** Comment on which method you found easier.

45. Consider the following set property: For all sets A, B, and C, $(A - B) \cup (B - C) = (A \cup B) - (B \cap C)$.
- **a.** Use an element argument to derive the property.
- **b.** Use an algebraic argument to derive the property (by applying properties from Theorem 6.2.2).
- **c.** Comment on which method you found easier.

Definition: Given sets A and B, the **symmetric difference of A and B**, denoted $A \Delta B$, is

$$A \Delta B = (A - B) \cup (B - A).$$

46. Let $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$, and $C = \{5, 6, 7, 8\}$. Find each of the following sets:
- **a.** $A \Delta B$
- **b.** $B \Delta C$
- **c.** $A \Delta C$
- **d.** $(A \Delta B) \Delta C$

Refer to the definition of symmetric difference given above. Prove each of 47–52, assuming that A, B, and C are all subsets of a universal set U.

47. $A \Delta B = B \Delta A$

48. $A \Delta \varnothing = A$

49. $A \Delta A^c = U$

50. $A \Delta A = \varnothing$

*H** **51.** If $A \Delta C = B \Delta C$, then $A = B$.

*H** **52.** $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

H **53.** Derive the set identity $A \cup (A \cap B) = A$ from the properties listed in Theorem 6.2.2(1)–(9). Start by showing that for every subset B of a universal set U, $U \cup B = U$. Then intersect both sides with A and deduce the identity.

54. Derive the set identity $A \cap (A \cup B) = A$ from the properties listed in Theorem 6.2.2(1)–(9). Start by showing that for every subset B of a universal set U, $\varnothing = \varnothing \cap B$. Then take the union of both sides with A and deduce the identity.

ANSWERS FOR TEST YOURSELF

1. make the left-hand side unequal to the right-hand side (*Or: result in different values on the two sides of the equation*) **2.** cite one of the properties from Theorem 6.2.2 (*Or: give a precise reason*) **3.** exactly

6.4 Boolean Algebras, Russell's Paradox, and the Halting Problem

From the paradise created for us by Cantor, no one will drive us out.
—David Hilbert (1862–1943)

Table 6.4.1 summarizes the main features of the logical equivalences from Theorem 2.1.1 and the set properties from Theorem 6.2.2. Notice how similar the entries in the two columns are.

TABLE 6.4.1

Logical Equivalences	**Set Properties**
For all statement variables p, q, and r:	For all sets A, B, and C:
a. $p \vee q \equiv q \vee p$ b. $p \wedge q \equiv q \wedge p$	a. $A \cup B = B \cup A$ b. $A \cap B = B \cap A$
a. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ b. $p \vee (q \vee r) \equiv (p \vee q) \vee r$	a. $A \cap (B \cap C) = (A \cap B) \cap C$ b. $A \cup (B \cup C) = (A \cup B) \cup C$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \varnothing = A$ b. $A \cap U = A$
a. $p \vee \sim p \equiv \mathbf{t}$ b. $p \wedge \sim p \equiv \mathbf{c}$	a. $A \cup A^c = U$ b. $A \cap A^c = \varnothing$
$\sim(\sim p) \equiv p$	$(A^c)^c = A$
a. $p \vee p \equiv p$ b. $p \wedge p \equiv p$	a. $A \cup A = A$ b. $A \cap A = A$
a. $p \vee \mathbf{t} \equiv \mathbf{t}$ b. $p \wedge \mathbf{c} \equiv \mathbf{c}$	a. $A \cup U = U$ b. $A \cap \varnothing = \varnothing$
a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$	a. $(A \cup B)^c = A^c \cap B^c$ b. $(A \cap B)^c = A^c \cup B^c$
a. $p \vee (p \wedge q) \equiv p$ b. $p \wedge (p \vee q) \equiv p$	a. $A \cup (A \cap B) = A$ b. $A \cap (A \cup B) = A$
a. $\sim\mathbf{t} \equiv \mathbf{c}$ b. $\sim\mathbf{c} \equiv \mathbf{t}$	a. $U^c = \varnothing$ b. $\varnothing^c = U$

If you let $\vee$ (*or*) correspond to $\cup$ (union), $\wedge$ (*and*) correspond to $\cap$ (intersection), **t** (a tautology) correspond to U (a universal set), **c** (a contradiction) correspond to $\varnothing$ (the empty set), and $\sim$ (negation) correspond to ^{c} (complementation), then you can see that the structure of the set of statement forms with operations $\vee$ and $\wedge$ is essentially identical to the structure of the set of subsets of a universal set with operations $\cup$ and $\cap$. In fact, both are special cases of the same general structure, known as a *Boolean algebra*. The essential idea of a Boolean algebra was introduced by the self-taught English mathematician/logician George Boole in 1847 in a book entitled *The Mathematical Analysis of Logic*. During the remainder of the nineteenth century, Boole and others amplified and clarified the concept until it reached the form in which we use it today.

In this section we show how to derive the various properties associated with a Boolean algebra from a set of five axioms.

Definition and Axioms for a Boolean Algebra

A **Boolean algebra** is a set B together with two operations, generally denoted $+$ and $\cdot$, such that for all a and b in B both $a+b$ and $a\cdot b$ are in B and the following axioms are assumed to hold:

1. *Commutative Laws:* For all a and b in B,

   $$\text{(a) } a+b=b+a \quad \text{and} \quad \text{(b) } a\cdot b=b\cdot a.$$

2. *Associative Laws:* For all a, b, and c in B,

   $$\text{(a) } (a+b)+c=a+(b+c) \quad \text{and} \quad \text{(b) } (a\cdot b)\cdot c=a\cdot(b\cdot c).$$

3. *Distributive Laws:* For all a, b, and c in B,

   $$\text{(a) } a+(b\cdot c)=(a+b)\cdot(a+c) \quad \text{and} \quad \text{(b) } a\cdot(b+c)=(a\cdot b)+(a\cdot c).$$

4. *Identity Laws:* There exist distinct elements 0 and 1 in B such that for each a in B,

   $$\text{(a) } a+0=a \quad \text{and} \quad \text{(b) } a\cdot 1=a.$$

5. *Complement Laws:* For each a in B, there exists an element in B, denoted $\overline{a}$ and called the **complement** or **negation** of a, such that

   $$\text{(a) } a+\overline{a}=1 \quad \text{and} \quad \text{(b) } a\cdot\overline{a}=0.$$

In any Boolean algebra, the complement of each element is unique, the quantities 0 and 1 are unique, and identities analogous to those in Theorem 2.1.1 and Theorem 6.2.2 can be deduced.

Theorem 6.4.1 Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Laws:* For all a and x in B, if $a+x=1$ and $a\cdot x=0$ then $x=\overline{a}$.
2. *Uniqueness of* 0 *and* 1: If there exists x in B such that $a+x=a$ for every a in B, then $x=0$, and if there exists y in B such that $a\cdot y=a$ for every a in B, then $y=1$.
3. *Double Complement Law:* For every $a\in B$, $(\overline{\overline{a}})=a$.
4. *Idempotent Laws:* For every $a\in B$,

   $$\text{(a) } a+a=a \quad \text{and} \quad \text{(b) } a\cdot a=a.$$

5. *Universal Bound Laws:* For every $a\in B$,

   $$\text{(a) } a+1=1 \quad \text{and} \quad \text{(b) } a\cdot 0=0.$$

6. *De Morgan's Laws:* For all a and $b\in B$,

   $$\text{(a) } \overline{a+b}=\overline{a}\cdot\overline{b} \quad \text{and} \quad \text{(b) } \overline{a\cdot b}=\overline{a}+\overline{b}.$$

7. *Absorption Laws:* For all a and $b \in B$,

$$\text{(a) } (a + b)\cdot a = a \quad \text{and} \quad \text{(b) } (a\cdot b) + a = a.$$

8. *Complements of* 0 *and* 1:

$$\text{(a) } \overline{0} = 1 \quad \text{and} \quad \text{(b) } \overline{1} = 0.$$

Proof:

Part 1: Uniqueness of the Complement Law
Suppose a and x are particular, but arbitrarily chosen, elements of B that satisfy the following hypothesis: $a + x = 1$ and $a\cdot x = 0$. Then

$x = x\cdot 1$	because 1 is an identity for $\cdot$
$= x\cdot(a + \overline{a})$	by the complement law for $+$
$= x\cdot a + x\cdot\overline{a}$	by the distributive law for $\cdot$ over $+$
$= a\cdot x + x\cdot\overline{a}$	by the commutative law for $\cdot$
$= 0 + x\cdot\overline{a}$	by hypothesis
$= a\cdot\overline{a} + x\cdot\overline{a}$	by the complement law for $\cdot$
$= (\overline{a}\cdot a) + (\overline{a}\cdot x)$	by the commutative law for $\cdot$
$= \overline{a}\cdot(a + x)$	by the distributive law for $\cdot$ over $+$
$= \overline{a}\cdot 1$	by hypothesis
$= \overline{a}$	because 1 is an identity for $\cdot$.

Proofs of the other parts of the theorem are discussed in the examples that follow and in the exercises.

You may notice that all parts of the definition of a Boolean algebra and most parts of Theorem 6.4.1 contain paired statements. For instance, the distributive laws state that for all a, b, and c in B,

$$\text{(a) } a + (b\cdot c) = (a + b)\cdot(a + c) \quad \text{and} \quad \text{(b) } a\cdot(b + c) = (a\cdot b) + (a\cdot c),$$

and the identity laws state that for every a in B,

$$\text{(a) } a + 0 = a \quad \text{and} \quad \text{(b) } a\cdot 1 = a.$$

Each of the paired statements can be obtained from the other by interchanging all the $+$ and $\cdot$ signs and interchanging 1 and 0. Such interchanges transform any Boolean identity into its **dual** identity. It can be proved that the dual of any Boolean identity is also an identity. This fact is often called the **duality principle** for a Boolean algebra.

Example 6.4.1 **Proof of the Double Complement Law**

Prove that for all elements a in a Boolean algebra B, $\overline{(\overline{a})} = a$.

Solution Start by supposing that B is a Boolean algebra and a is any element of B. The basis for the proof is the uniqueness of the complement law: that each element in B has a unique complement, which satisfies certain equations with respect to it. So if a can be shown to satisfy those equations with respect to $\overline{a}$, then a must be the complement of $\overline{a}$.

Theorem 6.4.1(3) Double Complement Law

For every element a in a Boolean algebra B, $\overline{(\overline{a})} = a$.

Proof:

Suppose B is a Boolean algebra and a is any element of B. Then

$$\begin{aligned} \overline{a} + a &= a + \overline{a} && \text{by the commutative law for } + \\ &= 1 && \text{by the complement law for 1} \end{aligned}$$

and

$$\begin{aligned} \overline{a} \cdot a &= a \cdot \overline{a} && \text{by the commutative law for.} \\ &= 0 && \text{by the complement law for 0.} \end{aligned}$$

Thus a satisfies the two equations with respect to $\overline{a}$ that are satisfied by the complement of $\overline{a}$. From the fact that the complement of a is unique, we conclude that $\overline{(\overline{a})} = a$.

■

Example 6.4.2 **Proof of an Idempotent Law**

Fill in the blanks in the following proof that for all elements a in a Boolean algebra B, $a + a = a$.

Proof:

Suppose B is a Boolean algebra and a is any element of B. Then

$$\begin{aligned} a &= a + 0 && \underline{\text{(a)}} \\ &= a + (a \cdot \overline{a}) && \underline{\text{(b)}} \\ &= (a + a) \cdot (a + \overline{a}) && \underline{\text{(c)}} \\ &= (a + a) \cdot 1 && \underline{\text{(d)}} \\ &= a + a && \underline{\text{(e)}}. \end{aligned}$$

Solution

(a) because 0 is an identity for +

(b) by the complement law for ·

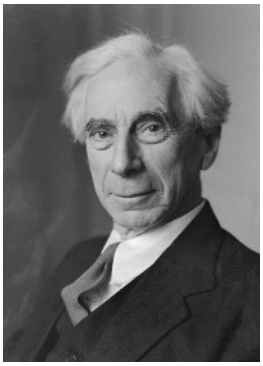
(c) by the distributive law for + over ·

(d) by the complement law for +

(e) because 1 is an identity for ·

■

Russell's Paradox



Bettmann/Getty Images

Bertrand Russell (1872–1970)

By the beginning of the twentieth century, abstract set theory had gained such wide acceptance that a number of mathematicians were working hard to show that all of mathematics could be built upon a foundation of set theory. In the midst of this activity, the English mathematician and philosopher Bertrand Russell discovered a "paradox" (really a genuine contradiction) that seemed to shake the very core of the foundation. The paradox assumes Cantor's definition of set as "any collection into a whole of definite and separate objects of our intuition or our thought."

Russell's Paradox: Most sets are not elements of themselves. For instance, the set of all integers is not an integer and the set of all horses is not a horse. However, we can imagine the possibility of a set's being an element of itself. For instance, the set of all abstract ideas might be considered an abstract idea. If we are allowed to use any description of a property as the defining property of a set, we can let S be the set of all sets that are not elements of themselves:

$$S = \{A \mid A \text{ is a set and } A \notin A\}.$$

Is S an element of itself?

The answer is both yes and no. For suppose $S \in S$. Then S satisfies the defining property for S, and hence $S \notin S$. This contradicts the supposition that $S \in S$ and shows that $S \notin S$. Next suppose $S \notin S$. Then S is a set such that $S \notin S$ and so S satisfies the defining property for S, which implies that $S \in S$. This contradicts the supposition that $S \notin S$ and shows that $S \in S$. Thus both $S \in S$ and $S \notin S$, which is impossible because a statement is either true or false but not both. To help explain his discovery to laypeople, Russell devised a puzzle, the barber puzzle, whose solution exhibits the same logic as his paradox.

Example 6.4.3 **The Barber Puzzle**

In a certain town there is a male barber who shaves all those men, and only those men, who do not shave themselves. *Question:* Does the barber shave himself?

Solution The answer is both yes and no. If the barber shaves himself, he is a member of the class of men who shave themselves. But no member of this class is shaved by the barber, and so the barber does *not* shave himself. On the other hand, if the barber does not shave himself, he belongs to the class of men who do not shave themselves. But the barber shaves every man in this class, so the barber *does* shave himself. ■

How can the answer be both yes and no? Surely any barber either does or does not shave himself. You might try to think of circumstances that would make the paradox disappear. For instance, maybe the barber happens to have no beard and never shaves. But a condition of the puzzle is that the barber is a man who shaves *all* those men who do not shave themselves. If he does not shave, then he does not shave himself, in which case he is shaved by the barber and the contradiction is as present as ever. Other attempts at resolving the paradox by considering details of the barber's situation are similarly doomed to failure.

So let's accept the fact that the paradox has no easy resolution and see where that thought leads. Since the barber both shaves himself and doesn't shave himself, the sentence "The barber shaves himself" is both true and false. Yet the sentence arose in a natural way from a description of a situation. If the situation actually existed, then the sentence would have to be either true or false but not both. Thus we are forced to conclude that the situation described in the puzzle simply cannot exist in the world as we know it.

In a similar way, the conclusion to be drawn from Russell's paradox itself is that the object S is not a set. Because if it actually were a set, in the sense of satisfying the general properties of sets that we have been assuming, then it either would be an element of itself or not.

In the years following Russell's discovery, several ways were found to define the basic concepts of set theory so as to avoid his contradiction. The way used in this text requires that, except for the power set whose existence is guaranteed by an axiom, whenever a set is defined using a predicate as a defining property, the stipulation must also be made that the set is a subset of a known set. This method does not allow us to talk about "the set of all sets that are not elements of themselves." We can speak only of "the set of all sets that are subsets of some known set and that are not elements of themselves." When this restriction is made, Russell's paradox ceases to be contradictory. Here is what happens:

Let U be a universal set and suppose that all sets under discussion are subsets of U. Let

$$S = \{A \mid A \subseteq U \text{ and } A \notin A\}.$$

In Russell's paradox, both implications

$$S \in S \rightarrow S \notin S \quad \text{and} \quad S \notin S \rightarrow S \in S$$

are proved, and the contradictory conclusion

$$\text{both } S \in S \quad \text{and} \quad S \notin S$$

is therefore deduced. In the situation in which all sets under discussion are subsets of U, the implication $S \in S \rightarrow S \notin S$ is proved in almost the same way as it is for Russell's paradox: (Suppose $S \in S$. Then by definition of S, $S \subseteq U$ and $S \notin S$. In particular, $S \notin S$.) On the other hand, from the supposition that $S \notin S$ we can only deduce that the statement "$S \subseteq U$ and $S \notin S$" is false. By one of De Morgan's laws, this means that "$S \not\subseteq U$ or $S \in S$." Since $S \in S$ would contradict the supposition that $S \notin S$, we eliminate it and conclude that $S \not\subseteq U$. In other words, the only conclusion we can draw is that the seeming "definition" of S is faulty—in other words, S is not a set in U.

Pictorial Press Ltd./Alamy Stock Photo

Kurt Gödel (1906–1978)

Russell's discovery had a profound impact on mathematics because even though his contradiction could be made to disappear by more careful definitions, its existence caused people to wonder whether other contradictions remained. In 1931 Kurt Gödel showed that it is not possible to prove, in a mathematically rigorous way, that mathematics is free of contradictions. You might think that Gödel's result would have caused mathematicians to give up their work in despair, but that has not happened. On the contrary, there has been more mathematical activity since 1931 than in any other period in history.

The Halting Problem

Well before the actual construction of an electronic computer, Alan M. Turing (1912–1954) deduced a profound theorem about how such computers would have to work. The argument he used is similar to that in Russell's paradox. It is also related to those used by Gödel to prove his theorem and by Cantor to prove that it is impossible to write all the real numbers in an infinitely long list, even given an infinitely long period of time (see Section 7.4).

If you have some experience programming computers, you know how badly an infinite loop can tie up a computer system. It would be useful to be able to preprocess a program and its data set by running it through a checking program that determines whether execution of the given program with the given data set would result in an infinite loop. Can an algorithm for such a program be written? In other words, can an algorithm be written that will accept any algorithm X and any data set D as input and will then print

"halts" or "loops forever" to indicate whether X terminates in a finite number of steps or loops forever when run with data set D? In the 1930s, Turing proved that the answer to this question is no.

Theorem 6.4.2

There is no computer algorithm that will accept any algorithm X and data set D as input and then will output "halts" or "loops forever" to indicate whether or not X terminates in a finite number of steps when X is run with data set D.

Proof (by contradiction):

Suppose there is an algorithm, CheckHalt, such that if an algorithm X and a data set D are input, then

CheckHalt(X, D) prints

"halts" if X terminates in a finite number of steps when run with data set D

or

"loops forever" if X does not terminate in a finite number of steps when run with data set D.

[To show that no algorithm such as CheckHalt can exist, we will deduce a contradiction.]

Observe that the sequence of characters making up an algorithm X can be regarded as a data set itself. Thus it is possible to consider running CheckHalt with input (X, X). Define a new algorithm, Test, as follows: For any input algorithm X,

Test(X)

loops forever if CheckHalt(X, X) prints "halts"

or

stops if CheckHalt(X, X) prints "loops forever".

Now run algorithm Test with input Test. If Test(Test) terminates after a finite number of steps, then the value of CheckHalt(Test, Test) is "halts" and so Test(Test) loops forever.

On the other hand, if Test(Test) does not terminate after a finite number of steps, then CheckHalt(Test, Test) prints "loops forever" and so Test(Test) terminates.

The two paragraphs above show that Test(Test) loops forever and also that it terminates. This is a contradiction. But the existence of Test follows logically from the supposition of the existence of an algorithm CheckHalt that can check any algorithm and data set for termination. *[Hence the supposition must be false, and there is no such algorithm.]*

The axioms introduced into set theory to avoid Russell's paradox are not entirely adequate to deal with the full range of recursively defined objects in computer algorithms. One response has been to develop an extension of set theory that includes new objects called hypersets. In addition, the kinds of semantic issues raised by the barber paradox are related to problems involved in processing natural language by computers.

TEST YOURSELF

1. In the comparison between the structure of the set of statement forms and the set of subsets of a universal set, the *or* operation $\vee$ corresponds to _____, the *and* operation $\wedge$ corresponds to _____, a tautology **t** corresponds to _____, a contradiction **c** corresponds to _____, and the negation operation, denoted $\sim$, corresponds to _____.

2. The operations of $+$ and $\cdot$ in a Boolean algebra are generalizations of the operations of _____ and _____ in the set of all statement forms in a given finite number of variables and the operations of _____ and _____ in the set of all subsets of a given set.

3. Russell showed that the following proposed "set definition" could not actually define a set: _____.

EXERCISE SET 6.4

In 1–3 assume that B is a Boolean algebra with operations $+$ and $\cdot$. Give the reasons needed to fill in the blanks in the proofs using only the axioms for a Boolean algebra.

1. *Idempotent law for $\cdot$:* For every a in B, $a \cdot a = a$.
Proof: Let a be any element of B. Then

$$\begin{aligned} a &= a \cdot 1 && \text{(a)} \\ &= a \cdot (a + \bar{a}) && \text{(b)} \\ &= (a \cdot a) + (a \cdot \bar{a}) && \text{(c)} \\ &= (a \cdot a) + 0 && \text{(d)} \\ &= a \cdot a && \text{(e)}. \end{aligned}$$

2. *Universal bound law for $+$:* For every a in B, $a + 1 = 1$.
Proof: Let a be any element of B. Then

$$\begin{aligned} a + 1 &= a + (a + \bar{a}) && \text{(a)} \\ &= (a + a) + \bar{a} && \text{(b)} \\ &= a + \bar{a} && \text{by Example 6.4.2} \\ &= 1 && \text{(c)}. \end{aligned}$$

3. *Absorption law for $\cdot$ over $+$:* For all a and b in B, $(a + b) \cdot a = a$.
Proof: Let a be any element of B. Then

$$\begin{aligned} (a + b) \cdot a &= a \cdot (a + b) && \text{(a)} \\ &= a \cdot a + a \cdot b && \text{(b)} \\ &= a + a \cdot b && \text{by exercise 1} \\ &= a \cdot 1 + a \cdot b && \text{(c)} \\ &= a \cdot (1 + b) && \text{(d)} \\ &= a \cdot (b + 1) && \text{(e)} \\ &= a \cdot 1 && \text{by exercise 2} \\ &= a && \text{(f)}. \end{aligned}$$

In 4–10 assume that B is a Boolean algebra with operations $+$ and $\cdot$. Prove each statement using only the axioms for a Boolean algebra and statements proved in the text or in lower-numbered exercises.

4. *Universal bound for 0:* For every a in B, $a \cdot 0 = 0$.

5. *Complements of 0 and 1:*
   a. $\bar{0} = 1$ b. $\bar{1} = 0$

6. *Uniqueness of 0:* There is only one element of B that is an identity for $+$.

H 7. *Uniqueness of 1:* There is only one element of B that is an identity for $\cdot$.

8. *De Morgan's law for $\cdot$:* For all a and b in B, $\overline{a \cdot b} = \bar{a} + \bar{b}$. (*Hint:* Prove that $(a \cdot b) + (\bar{a} + \bar{b}) = 1$ and that $(a \cdot b) + (\bar{a} + \bar{b}) = 0$, and use the fact that $a \cdot b$ has a unique complement.)

9. *De Morgan's law for $+$:* For all a and b in B, $\overline{a + b} = \bar{a} \cdot \bar{b}$.

H 10. *Cancellation law:* For all x, y, and z in B, if $x + y = x + z$ and $x \cdot y = x \cdot z$, then $y = z$.

11. Let $S = \{0, 1\}$, and define operations $+$ and $\cdot$ on S by the following tables:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

   a. Show that the elements of S satisfy the following properties:
   (i) the commutative law for $+$
   (ii) the commutative law for $\cdot$
   (iii) the associative law for $+$
   (iv) the associative law for $\cdot$
   H (v) the distributive law for $+$ over $\cdot$
   (vi) the distributive law for $\cdot$ over $+$

H b. Show that 0 is an identity element for $+$ and that 1 is an identity element for $\cdot$.

c. Define $\overline{0} = 1$ and $\overline{1} = 0$. Show that for every a in S, $a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$. It follows from parts (a)–(c) that S is a Boolean algebra with the operations $+$ and $\cdot$.

Exercises 12–15 provide an outline for a proof that the associative laws, which were included as an axiom for a Boolean algebra, can be derived from the other four axioms. The outline is from *Introduction to Boolean Algebra* by S. Givant and P. Halmos, Springer, 2009. In order to avoid unneeded parentheses, assume that $\cdot$ takes precedence over $+$.

12. The universal bound law for $+$ states that for every element a in a Boolean algebra, $a + 1 = 1$. The proof shown in exercise 2 used the associative law for $+$. Rederive the law without using the associative law and using only the other four axioms for a Boolean algebra.

H 13. The absorption law for $+$ states that for all elements a and b in a Boolean algebra, $a \cdot b + a = a$. Prove this law without using the associative law and using only the other four axioms for a Boolean algebra plus the result of exercise 12.

14. *Test for equality law:* For all elements a, b, and c in a Boolean algebra,

If $b \cdot a = c \cdot a$ and $b \cdot \overline{a} = c \cdot \overline{a}$, then $b = c$.

Without using the associative law, derive this law from the other four laws in the axioms for a Boolean algebra plus the result of exercise 12.

H 15. The associative law for $+$ states that for all elements a, b, and c in a Boolean algebra, $a + (b + c) = (a + b) + c$. Show that this law, as well as the associative law for $\cdot$, can be derived from the other four axioms in the definition and axioms for a Boolean algebra. Then explain how to use your work to obtain a derivation for the associative law for $\cdot$.

Hints: To prove this theorem, suppose a, b, and c are any elements in a Boolean algebra B, and divide the proof into three parts. ***Part 1:*** Prove that $(a + (b + c)) \cdot a = ((a + b) + c) \cdot a$. ***Part 2:*** Prove that $(a + (b + c)) \cdot \overline{a} = ((a + b) + c) \cdot \overline{a}$. ***Part 3:*** Use the results of parts 1 and 2 to prove that $a + (b + c) = (a + b) + c$. You may use the universal bound law for $+$, the absorption law for $+$, and the test for equality law from exercises 12, 13, and 14 because the associative laws were not used to derive these properties.

In 16–21 determine whether each sentence is a statement. Explain your answers.

16. This sentence is false.

17. If $1 + 1 = 3$, then $1 = 0$.

18. The sentence in this box is a lie.

19. All positive integers with negative squares are prime.

20. This sentence is false or $1 + 1 = 3$.

21. This sentence is false and $1 + 1 = 2$.

22. a. Assuming that the following sentence is a statement, prove that $1 + 1 = 3$:

If this sentence is true, then $1 + 1 = 3$.

b. What can you deduce from part (a) about the status of "This sentence is true"? Why? (This example is known as **Löb's paradox**.)

H 23. The following two sentences were devised by the logician Saul Kripke. While not intrinsically paradoxical, they could be paradoxical under certain circumstances. Describe such circumstances.

(i) Most of Nixon's assertions about Watergate are false.

(ii) Everything Jones says about Watergate is true.

(*Hint:* Suppose Nixon says (ii) and the only utterance Jones makes about Watergate is (i).)

24. Can there exist a computer program that has as output a list of all the computer programs that do not list themselves in their output? Explain your answer.

25. Can there exist a book that refers to all those books and only those books that do not refer to themselves? Explain your answer.

26. Some English adjectives are descriptive of themselves (for instance, the word *polysyllabic* is polysyllabic) whereas others are not (for instance, the word *monosyllabic* is not monosyllabic). The word *heterological* refers to an adjective that does not describe itself. Is *heterological* heterological? Explain your answer.

27. As strange as it may seem, it is possible to give a precise-looking verbal definition of an integer that, in fact, is not a definition at all. The following was devised by an English librarian, G. G. Berry, and reported by Bertrand Russell. Explain how it leads

to a contradiction. Let n be "the smallest integer not describable in fewer than 12 English words." (Note that the total number of strings consisting of 11 or fewer English words is finite.)

***H* 28.** Is there an algorithm which, for a fixed quantity a and any input algorithm X and data set D, can determine whether X prints a when run with data set D? Explain. (This problem is called the **printing problem**.)

29. Use a technique similar to that used to derive Russell's paradox to prove that for any set A, $\mathcal{P}(A) \not\subseteq A$.

ANSWERS FOR TEST YOURSELF

1. the operation of union $\cup$; the operation of intersection $\cap$; a universal set U; the empty set $\varnothing$; the operation of complementation, denoted by using the superscript c **2.** $\vee$; $\wedge$; $\cup$; $\cap$ **3.** the set of all sets that are not elements of themselves

CHAPTER 7 PROPERTIES OF FUNCTIONS

The concept of function is essential in all areas of mathematics and computer science. Earlier in this book we discussed sequences (which are functions defined on sets of integers), *mod* and *div* (which are functions defined on Cartesian products of integers), floor and ceiling (which are functions from **R** to **Z**), and truth tables and input/output tables (which can be regarded as Boolean functions).

In this chapter we consider an additional wide variety of functions, focusing on those defined on discrete sets (such as finite sets or sets of integers). We then look at properties of functions such as one-to-one and onto, existence of inverse functions, and the interaction of composition of functions and the properties of one-to-one and onto. We end the chapter with the surprising result that there are different sizes of infinite sets and give an application to computability.

7.1 Functions Defined on General Sets

The theory that has had the greatest development in recent times is without any doubt the theory of functions. —Vito Volterra, 1888

As used in ordinary language, the word *function* indicates dependence of one varying quantity on another. If your teacher tells you that your grade in a course will be a function of your performance on the exams, you interpret this to mean that the teacher has some rule for translating exam scores into grades. To each collection of exam scores there corresponds a certain grade.

In Section 1.3 we defined a function as a certain type of relation. In this chapter we focus on the more dynamic way functions are used in mathematics. The following is a restatement of the definition of function that includes additional terminology associated with the concept.

Definition

A **function f from a set X to a set Y**, denoted $f: X \to Y$, is a relation from X, the **domain** of f, to Y, the **co-domain** of f, that satisfies two properties: (1) every element in X is related to some element in Y, and (2) no element in X is related to more than one element in Y. Thus, given any element x in X, there is a unique element in Y that is related to x by f. If we call this element y, then we say that "f sends x to y" or "f maps x to y" and write $x \xrightarrow{f} y$ or $f: x \to y$. The unique element to which f sends x is denoted

$$f(x) \quad \text{and is called} \quad \begin{array}{l} \textbf{f of x}, \text{ or} \\ \textbf{the output of f for the input x}, \text{ or} \\ \textbf{the value of f at x}, \text{ or} \\ \textbf{the image of x under f}. \end{array}$$

The set of all values of f taken together is called the *range of f* or the *image of X under f*. Symbolically:

$$\textbf{range of } f = \textbf{image of } X \textbf{ under } f = \{y \in Y \mid y = f(x), \text{ for some } x \text{ in } X\}.$$

Given an element y in Y, there may exist elements in X with y as their image. When x is an element such that $f(x) = y$, then x is called **a preimage of y** or **an inverse image of y**. The set of all inverse images of y is called *the inverse image of y*. Symbolically:

$$\textbf{the inverse image of } y = \{x \in X \mid f(x) = y\}.$$

Caution! Use $f(x)$ to refer to the value of the function f at x. Generally avoid using $f(x)$ to refer to the function f itself.

INTERFOTO/Alamy Stock Photo

Johann Peter Gustav Lejeune Dirichlet (1805–1859)

In some mathematical contexts, the notation $f(x)$ is used to refer both to the value of f at x and to the function f itself. Because using the notation this way can lead to confusion, we avoid it whenever possible. In this book, unless explicitly stated otherwise, the symbol $f(x)$ always refers to the value of the function f at x and not to the function f itself.

The concept of function was developed over a period of centuries. A definition similar to that given above was first formulated for sets of numbers by the German mathematician Lejeune Dirichlet (DEER-ish-lay) in 1837.

Arrow Diagrams

Recall from Section 1.3 that if X and Y are finite sets, you can define a function f from X to Y by drawing an arrow diagram. You make a list of elements in X and a list of elements in Y, and draw an arrow from each element in X to the corresponding element in Y, as shown in Figure 7.1.1.

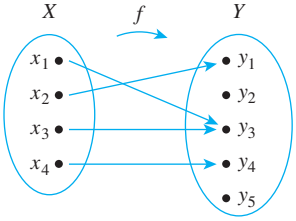


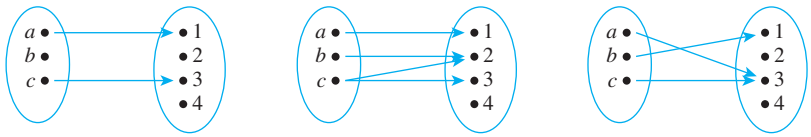
FIGURE 7.1.1

This arrow diagram does define a function because:

1. Every element of X has an arrow that points to an element in Y.
2. No element of X has two arrows that point to two different elements of Y.

Example 7.1.1 **Functions and Nonfunctions**

Which of the arrow diagrams in Figure 7.1.2 define functions from $X = \{a, b, c\}$ to $Y = \{1, 2, 3, 4\}$?



(a) (b) (c)

FIGURE 7.1.2

Solution Only (c) defines a function. In (a) the element b in X is not related to any element of Y because there is no arrow that points from b to an element in Y. And in (b) the element c is not related to a *unique* element of Y because from c there are two arrows that point to two different elements of Y—one toward 2 and the other toward 3. ■

Example 7.1.2 **A Function Defined by an Arrow Diagram**

Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$. Define a function f from X to Y by the arrow diagram in Figure 7.1.3.

a. Write the domain and co-domain of f.

b. Find $f(a)$, $f(b)$, and $f(c)$.

c. What is the range of f?

d. Is c an inverse image of 2? Is b an inverse image of 3?

e. Find the inverse images of 2, 4, and 1.

f. Represent f as a set of ordered pairs.

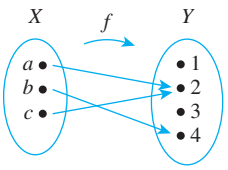


FIGURE 7.1.3

Solution

a. domain of $f = \{a, b, c\}$, co-domain of $f = \{1, 2, 3, 4\}$

b. $f(a) = 2$, $f(b) = 4$, $f(c) = 2$

c. range of $f = \{2, 4\}$

d. yes, no

e. inverse image of $2 = \{a, c\}$
inverse image of $4 = \{b\}$
inverse image of $1 = \varnothing$ (*since no arrows point to* 1)

f. $\{(a, 2), (b, 4), (c, 2)\}$ ■

In Example 7.1.2 there are no arrows pointing from X to the 1 or the 3 in Y. This illustrates the fact that although each element of the domain of a function must have an arrow pointing out from it, there can be elements of the co-domain to which no arrows point. Note also that there are two arrows pointing to the 2—one coming from a and the other from c. This does not violate the definition of function.

In Section 1.3 we gave a test for determining whether two functions with the same domain and co-domain are equal, saying that the test results from the definition of a function as a relation. We formalize this justification in Theorem 7.1.1.

Theorem 7.1.1 A Test for Function Equality

If $F: X \to Y$ and $G: X \to Y$ are functions, then $F = G$ if, and only if, $F(x) = G(x)$ for every $x \in X$.

Note
$(x, y) \in F \Leftrightarrow y = F(x)$
$(x, y) \in G \Leftrightarrow y = G(x)$.

Proof: Suppose $F: X \to Y$ and $G: X \to Y$ are functions; that is, F and G are relations from X to Y that satisfy the two additional function properties. Then F and G are subsets of $X \times Y$, and for (x, y) to be in F means that y is the unique element related to x by F, which we denote as $F(x)$. Similarly, for (x, y) to be in G means that y is the unique element related to x by G, which we denote as $G(x)$.

Now suppose that $F(x) = G(x)$ for every $x \in X$. Then if x is any element of X,

$$(x, y) \in F \Leftrightarrow y = F(x) \Leftrightarrow y = G(x) \Leftrightarrow (x, y) \in G \qquad \text{because } F(x) = G(x).$$

So F and G consist of exactly the same elements and hence $F = G$.

Conversely, if $F = G$, then for every $x \in X$,

$$y = F(x) \Leftrightarrow (x, y) \in F \Leftrightarrow (x, y) \in G \Leftrightarrow y = G(x) \qquad \text{because } F \text{ and } G \text{ consist of exactly the same elements.}$$

Thus, since both $F(x)$ and $G(x)$ equal y, we have that

$$F(x) = G(x).$$

Example 7.1.3 **Equality of Functions**

a. Let $J_3 = \{0, 1, 2\}$, and define functions f and g from J_3 to J_3 as follows: For every x in J_3,

$$f(x) = (x^2 + x + 1) \bmod 3 \quad \text{and} \quad g(x) = (x + 2)^2 \bmod 3.$$

Does $f = g$?

b. Let $F: \mathbf{R} \to \mathbf{R}$ and $G: \mathbf{R} \to \mathbf{R}$ be functions. Define new functions $F + G: \mathbf{R} \to \mathbf{R}$ and $G + F: \mathbf{R} \to \mathbf{R}$ as follows: For every $x \in R$,

$$(F + G)(x) = F(x) + G(x) \quad \text{and} \quad (G + F)(x) = G(x) + F(x).$$

Does $F + G = G + F$?

Solution

a. Yes, the table of values shows that $f(x) = g(x)$ for every x in J_3.

x	$x^2 + x + 1$	$f(x) = (x^2 + x + 1) \bmod 3$	$(x + 2)^2$	$g(x) = (x + 2)^2 \bmod 3$
0	1	$1 \bmod 3 = 1$	4	$4 \bmod 3 = 1$
1	3	$3 \bmod 3 = 0$	9	$9 \bmod 3 = 0$
2	7	$7 \bmod 3 = 1$	16	$16 \bmod 3 = 1$

b. Again the answer is yes. For every real number x,

$$\begin{aligned} (F + G)(x) &= F(x) + G(x) && \text{by definition of } F + G \\ &= G(x) + F(x) && \text{by the commutative law for addition of real numbers} \\ &= (G + F)(x) && \text{by definition of } G + F. \end{aligned}$$

Hence $F + G = G + F$. ■

Examples of Functions

The following examples illustrate some of the wide variety of different types of functions.

Example 7.1.4 **The Identity Function on a Set**

Given a set X, define a function I_X from X to X by

$$I_X(x) = x \quad \text{for each } x \text{ in } X.$$

The function I_X is called the **identity function on X** because it sends each element of X to the element that is identical to it. Thus the identity function can be pictured as a machine that sends each piece of input directly to the output chute without changing it in any way.

Let X be any set, and suppose that a_{ij}^k and $\phi(z)$ are elements of X. Find $I_X\left(a_{ij}^k\right)$ and $I_X(\phi(z))$.

Solution Whatever is input to the identity function comes out unchanged, so $I_X\left(a_{ij}^k\right) = a_{ij}^k$ and $I_X(\phi(z)) = \phi(z)$. ■

Example 7.1.5 **Sequences**

The formal definition of sequences specifies that an infinite sequence is a function defined on the set of integers that are greater than or equal to a particular integer. For example, the sequence denoted

$$1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \ldots, \frac{(-1)^n}{n+1}, \ldots$$

can be thought of as the function f from the nonnegative integers to the real numbers that associates $0 \to 1$, $1 \to -\frac{1}{2}$, $2 \to \frac{1}{3}$, $3 \to -\frac{1}{4}$, $4 \to \frac{1}{5}$, and, in general, $n \to \frac{(-1)^n}{n+1}$. In other words, $f\colon \mathbf{Z}^{nonneg} \to \mathbf{R}$ is the function defined as follows:

$$\text{Send each integer } n \geq 0 \text{ to } f(n) = \frac{(-1)^n}{n+1}.$$

In fact, there are many functions that can be used to define a given sequence. For instance, express the sequence above as a function from the set of *positive* integers to the set of real numbers.

Solution Define $g : \mathbf{Z}^+ \to \mathbf{R}$ by $g(n) = \frac{(-1)^{n+1}}{n}$, for each $n \in \mathbf{Z}^+$. Then $g(1) = 1, g(2) = -\frac{1}{2}$, $g(3) = \frac{1}{3}$, and, in general,

$$g(n+1) = \frac{(-1)^{n+2}}{n+1} = \frac{(-1)^n}{n+1} = f(n).$$ ■

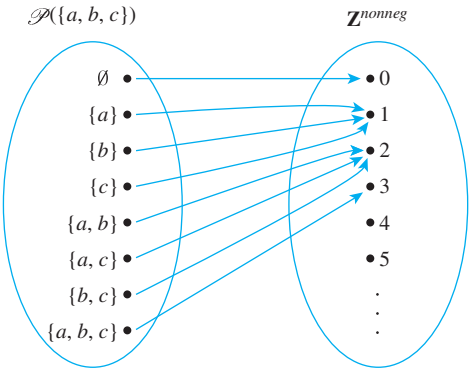
Example 7.1.6 **A Function Defined on a Power Set**

Recall from Section 6.1 that $\mathcal{P}(A)$ denotes the set of all subsets of the set A. Define a function $F\colon \mathcal{P}(\{a, b, c\}) \to \mathbf{Z}^{nonneg}$ as follows: For each $X \in \mathcal{P}(\{a, b, c\})$,

$$F(X) = \text{the number of elements in } X.$$

Draw an arrow diagram for F.

Solution



■

Example 7.1.7 **Functions Defined on a Cartesian Product**

Define functions $M: \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ and $R: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: For each ordered pair (a, b) of integers,

$$M(a, b) = ab \quad \text{and} \quad R(a, b) = (-a, b).$$

Note It is customary to omit one set of parentheses for functions defined on Cartesian products. For example, we write $M(a, b)$ rather than $M((a, b))$.

Then M is the multiplication function that sends each pair of real numbers to the product of the two, and R is the reflection function that sends each point in the plane that corresponds to a pair of real numbers to the mirror image of the point across the vertical axis. Find the following:

a. $M(-1, -1)$ b. $M\left(\frac{1}{2}, \frac{1}{2}\right)$ c. $M(\sqrt{2}, \sqrt{2})$

d. $R(2, 5)$ e. $R(-2, 5)$ f. $R(3, -4)$

Solution

a. $(-1)(-1) = 1$ b. $(1/2)(1/2) = 1/4$ c. $\sqrt{2} \cdot \sqrt{2} = 2$

d. $(-2, 5)$ e. $(-(-2), 5) = (2, 5)$ f. $(-3, -4)$ ■

Definition Logarithms and Logarithmic Functions

Let b be a positive real number with $b \neq 1$. For each positive real number x, the **logarithm with base b of x**, written $\log_b x$, is the exponent to which b must be raised to obtain x. Symbolically:

$$\log_b x = y \quad \Leftrightarrow \quad b^y = x.$$

The **logarithmic function with base b** is the function from $\mathbf{R}^+$ to $\mathbf{R}$ that takes each positive real number x to $\log_b x$.

Note It is not obvious, but it is true, that for any positive real number x there is a unique real number y such that $b^y = x$. Most calculus books contain a discussion of this result.

Example 7.1.8 **The Logarithmic Function with Base b**

Find the following:

a. $\log_3 9$ b. $\log_2\left(\frac{1}{2}\right)$ c. $\log_{10}(1)$ d. $\log_2(2^m)$ (m is any real number)

e. $2^{\log_2(m)}$ $(m > 0)$

Solution

a. $\log_3 9 = 2$ because $3^2 = 9$. b. $\log_2\left(\frac{1}{2}\right) = -1$ because $2^{-1} = \frac{1}{2}$.

c. $\log_{10}(1) = 0$ because $10^0 = 1$.

d. $\log_2(2^m) = m$ because the exponent to which 2 must be raised to obtain 2^m is m.

e. $2^{\log_2(m)} = m$ because $\log_2(m)$ is the exponent to which 2 must be raised to obtain m. ■

Recall that if S is a nonempty, finite set of characters, then a **string over S** can be regarded as a finite sequence of elements of S. The number of characters in a string is called the **length** of the string. The **null string over S** is the "string" with no characters. It is usually denoted λ and is said to have length 0.

Example 7.1.9 **Encoding and Decoding Functions**

Digital messages consist of finite sequences of 0's and 1's. When they are communicated across a transmission channel, they are frequently coded in special ways to reduce the possibility that they will be garbled by interfering noise in the transmission lines. For example, suppose a message consists of a sequence of 0's and 1's. A simple way to encode the message is to write each bit three times. Thus the message

$$00101111$$

would be encoded as

$$000000111000111111111111.$$

The receiver of the message decodes it by replacing each section of three identical bits by the one bit to which all three are equal.

Let A be the set of all strings of 0's and 1's, and let T be the set of all strings of 0's and 1's that consist of consecutive triples of identical bits. The encoding and decoding processes described above are actually functions from A to T and from T to A. The encoding function E is the function from A to T defined as follows: For each string $s \in A$,

$$E(s) = \text{the string obtained from } s \text{ by replacing each bit of } s \text{ by the same bit written three times.}$$

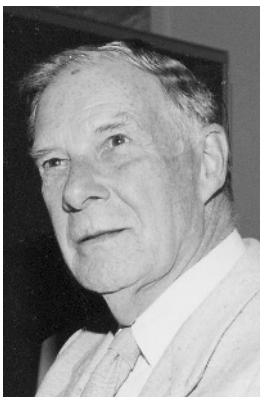
The decoding function D is defined as follows: For each string $t \in T$,

$$D(t) = \text{the string obtained from } t \text{ by replacing each consecutive triple of three identical bits of } t \text{ by a single copy of that bit.}$$

The advantage of this particular coding scheme is that it makes it possible to do a certain amount of error correction when interference in the transmission channels has introduced errors into the stream of bits. If the receiver of the coded message observes that one of the sections of three consecutive bits that should be identical does not consist of identical bits, then one bit differs from the other two. In this case, if errors are rare, it is likely that the single bit that is different is the one in error, and this bit is changed to agree with the other two before applying the decoding function. ■

Example 7.1.10 **The Hamming Distance Function**

The Hamming distance function, named after the computer scientist Richard W. Hamming, is very important in coding theory. It gives a measure of the "difference" between two strings of 0's and 1's that have the same length. Let S_n be the set of all strings of 0's and 1's



Courtesy of U.S. Naval Academy

Richard Hamming
(1915–1998)

of length n. Define a function $H: S_n \times S_n \to \mathbf{Z}^{nonneg}$ as follows: For each pair of strings $(s, t) \in S_n \times S_n$,

$$H(s, t) = \text{the number of positions in which } s \text{ and } t \text{ have different values.}$$

Thus, letting $n = 5$,

$$H(11111, 00000) = 5$$

because 11111 and 00000 differ in all five positions, whereas

$$H(11000, 00000) = 2$$

because 11000 and 00000 differ only in the first two positions.

a. Find $H(00101, 01110)$. b. Find $H(10001, 01111)$.

Solution

a. 3 b. 4 ■

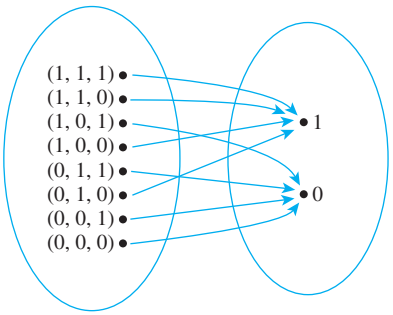
Boolean Functions

In Section 2.4 we showed how to find input/output tables for certain digital logic circuits. Any such input/output table defines a function in the following way: The elements in the input column can be regarded as ordered tuples of 0's and 1's; the set of all such ordered tuples is the domain of the function. The elements in the output column are all either 0 or 1; thus {0, 1} is taken to be the co-domain of the function. The relation sends each input element to the output element in the same row. Thus, for instance, the input/output table of Figure 7.1.4(a) defines the function with the arrow diagram shown in Figure 7.1.4(b).

More generally, the input/output table corresponding to a circuit with n input wires has n input columns. Such a table defines a function from the set of all n-tuples of 0's and 1's to the set {0, 1}.

Input			Output
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

(a)



(b)

FIGURE 7.1.4 Two Representations of a Boolean Function

Definition

An **(n-place) Boolean function** f is a function whose domain is the set of all ordered n-tuples of 0's and 1's and whose co-domain is the set {0, 1}. More formally, the domain of a Boolean function can be described as the Cartesian product of n copies of the set {0, 1}, which is denoted $\{0, 1\}^n$. Thus $f: \{0, 1\}^n \to \{0, 1\}$.

Example 7.1.11 **A Boolean Function**

Consider the three-place Boolean function defined from the set of all 3-tuples of 0's and 1's to {0, 1} as follows: For each triple (x_1, x_2, x_3) of 0's and 1's,

$$f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \ mod \ 2.$$

Describe f using an input/output table.

Solution

$$f(1, 1, 1) = (1 + 1 + 1) \ mod \ 2 = 3 \ mod \ 2 = 1$$

$$f(1, 1, 0) = (1 + 1 + 0) \ mod \ 2 = 2 \ mod \ 2 = 0$$

The rest of the values of f can be calculated similarly to obtain the following table.

Input			Output
x_1	x_2	x_3	$(x_1 + x_2 + x_3) \ mod \ 2$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

Checking Whether a Function Is Well Defined

It can sometimes happen that what appears to be a function defined by a rule is not really a function at all. To give an example, suppose we wrote, "Define a function f: $\mathbf{R} \rightarrow \mathbf{R}$ by specifying that for each real number x,

$$f(x) \text{ is the real number } y \text{ such that } x^2 + y^2 = 1."$$

There are two distinct reasons why this description does not define a function. For almost all values of x, either (1) there is no y that satisfies the given equation or (2) there are two different values of y that satisfy the equation. For instance, when $x = 2$, there is no real number y such that $2^2 + y^2 = 1$, and when $x = 0$, both $y = -1$ and $y = 1$ satisfy the equation $0^2 + y^2 = 1$. In general, we say that a "function" is **not well defined** if it fails to satisfy at least one of the requirements for being a function.

Example 7.1.12 **A Function That Is Not Well Defined**

Recall that $\mathbf{Q}$ represents the set of all rational numbers. Suppose you read that a function f: $\mathbf{Q} \rightarrow \mathbf{Z}$ is to be defined by the formula

$$f\left(\frac{m}{n}\right) = m \quad \text{for all integers } m \text{ and } n \text{ with } n \neq 0.$$

That is, the integer associated by f to the number $\frac{m}{n}$ is m. Is f well defined? Why?

Solution The function f is not well defined. The reason is that fractions have more than one representation as quotients of integers. For instance, $\frac{1}{2} = \frac{3}{6}$. Now if f were a function,

then the definition of a function would imply that $f\left(\frac{1}{2}\right) = \left(\frac{3}{6}\right)$ since $\frac{1}{2} = \frac{3}{6}$. But applying the formula for f, you find that

$$f\left(\frac{1}{2}\right) = 1 \quad \text{and} \quad f\left(\frac{3}{6}\right) = 3,$$

and so

$$f\left(\frac{1}{2}\right) \neq \left(\frac{3}{6}\right).$$

This contradiction shows that f is not well defined and, therefore, is not a function. ■

Note that the phrase *well-defined function* is actually redundant; for a function to be well defined really means that it is worthy of being called a function.

Functions Acting on Sets

Given a function from a set X to a set Y, you can consider the set of images in Y of all the elements in a subset of X and the set of inverse images in X of all the elements in a subset of Y.

Note For $y \in Y$, $f^{-1}(y) = f^{-1}(\{y\})$.

Definition

If $f: X \longrightarrow Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

$$f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \text{ in } A\}$$

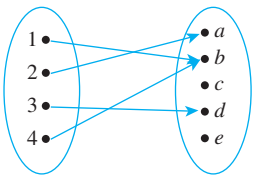
and

$$f^{-1}(C) = \{x \in X \mid f(x) \in C\}.$$

$f(A)$ is called the **image of A**, and $f^{-1}(C)$ is called the **inverse image of C**.

Example 7.1.13 **The Action of a Function on Subsets of a Set**

Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$, and define $F: X \longrightarrow Y$ by the following arrow diagram:



Let $A = \{1, 4\}$, $C = \{a, b\}$, and $D = \{c, e\}$. Find $F(A)$, $F(X)$, $F^{-1}(C)$, and $F^{-1}(D)$.

Solution

$$F(A) = \{b\} \quad F(X) = \{a, b, d\} \quad F^{-1}(C) = \{1, 2, 4\} \quad F^{-1}(D) = \varnothing$$

■

Example 7.1.14 **Interaction of a Function with Union**

Let X and Y be sets, let F be a function from X to Y, and let A and B be any subsets of X. Prove that $F(A \cup B) \subseteq F(A) \cup F(B)$.

Solution

The fact that X, Y, F, A, and B were formally introduced prior to the word "Prove" allows you to regard their existence and relationships as part of your background knowledge. Thus to prove that $F(A \cup B) \subseteq F(A) \cup F(B)$, you only need show that if y is any element in $F(A \cup B)$, then y is an element of $F(A) \cup F(B)$.

Proof:

Suppose $y \in F(A \cup B)$. *[We must show that* $y \in F(A) \cup F(B)$*.]* By definition of function, $y = F(x)$ for some $x \in A \cup B$. By definition of union, $x \in A$ or $x \in B$.

***Case 1*, $x \in A$:** In this case, $y = F(x)$ for some x in A. Hence $y \in F(A)$, and so by definition of union, $y \in F(A) \cup F(B)$.

***Case 2*, $x \in B$:** In this case, $y = F(x)$ for some x in B. Hence $y \in F(B)$, and so by definition of union, $y \in F(A) \cup F(B)$.

Thus in either case $y \in F(A) \cup F(B)$ *[as was to be shown].* ■

Exercise 40 asks you to prove the opposite containment from the one in Example 7.1.14. Taken together, the example and the solution to the exercise establish the full equality that $F(A \cup B) = F(A) \cup F(B)$.

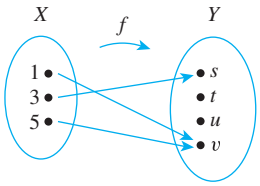
TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. Given a function f from a set X to a set Y, $f(x)$ is _____.
2. Given a function f from a set X to a set Y, if $f(x) = y$ then y is called _____ or _____ or _____.
3. Given a function f from a set X to a set Y, the range of f (or the image of X under f) is _____.
4. Given a function f from a set X to a set Y, if $f(x) = y$ then x is called _____ or _____.
5. Given a function f from a set X to a set Y, if $y \in Y$ then $f^{-1}(y) =$ _____ and is called _____.
6. Given functions f and g from a set X to a set Y, $f = g$ if, and only if, _____.
7. Given positive real numbers x and b with $b \neq 1$, $\log_b(x) =$ _____.
8. Given a function f from a set X to a set Y and a subset A of X, $f(A) =$ _____.
9. Given a function f from a set X to a set Y and a subset C of Y, $f^{-1}(C) =$ _____.

EXERCISE SET 7.1*

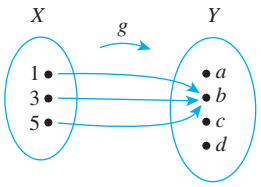
1. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$. Define $f: X \to Y$ by the following arrow diagram.



   a. Write the domain of f and the co-domain of f.
   b. Find $f(1)$, $f(3)$, and $f(5)$.
   c. What is the range of f?
   d. Is 3 an inverse image of s? Is 1 an inverse image of u?
   e. What is the inverse image of s? of u? of v?
   f. Represent f as a set of ordered pairs.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

2. Let $X = \{1, 3, 5\}$ and $Y = \{a, b, c, d\}$. Define $g : X \to Y$ by the following arrow diagram.



a. Write the domain of g and the co-domain of g.
b. Find $g(1)$, $g(3)$, and $g(5)$.
c. What is the range of g?
d. Is 3 an inverse image of a? Is 1 an inverse image of b?
e. What is the inverse image of b? of c?
f. Represent g as a set of ordered pairs.

3. Indicate whether the statements in parts (a)–(d) are true or false for all functions. Justify your answers.
a. If two elements in the domain of a function are equal, then their images in the co-domain are equal.
b. If two elements in the co-domain of a function are equal, then their preimages in the domain are also equal.
c. A function can have the same output for more than one input.
d. A function can have the same input for more than one output.

4. **a.** Find all functions from $X = \{a, b\}$ to $Y = \{u, v\}$.
b. Find all functions from $X = \{a, b, c\}$ to $Y = \{u\}$.
c. Find all functions from $X = \{a, b, c\}$ to $Y = \{u, v\}$.

5. Let $I_{\mathbf{Z}}$ be the identity function defined on the set of all integers, and suppose that e, b_i^{jk}, $K(t)$, and u_{kj} all represent integers. Find the following:
a. $I_{\mathbf{Z}}(e)$ **b.** $I_{\mathbf{Z}}(b_i^{jk})$ **c.** $I_{\mathbf{Z}}(K(t))$ **d.** $I_{\mathbf{Z}}(u_{kj})$

6. Find functions defined on the set of nonnegative integers that can be used to define the sequences whose first six terms are given below.
a. $1, -\frac{1}{3}, \frac{1}{5}, -\frac{1}{7}, \frac{1}{9}, -\frac{1}{11}$ **b.** $0, -2, 4, -6, 8, -10$

7. Let $A = \{1, 2, 3, 4, 5\}$, and define a function $F : \mathcal{P}(A) \to \mathbf{Z}$ as follows: For each set X in $\mathcal{P}(A)$,

$$F(X) = \begin{cases} 0 & \text{if } X \text{ has an even number of elements} \\ 1 & \text{if } X \text{ has an odd number of elements.} \end{cases}$$

Find the following:
a. $F(\{1, 3, 4\})$ **b.** $F(\varnothing)$
c. $F(\{2, 3\})$ **d.** $F(\{2, 3, 4, 5\})$

8. Let $J_5 = \{0, 1, 2, 3, 4\}$, and define a function $F : J_5 \to J_5$ as follows: For each $x \in J_5$, $F(x) = (x^3 + 2x + 4) \bmod 5$.
Find the following:
a. $F(0)$ **b.** $F(1)$ **c.** $F(2)$ **d.** $F(3)$ **e.** $F(4)$

9. Define a function $S : \mathbf{Z}^+ \to \mathbf{Z}^+$ as follows: For each positive integer n,

$S(n) =$ the sum of the positive divisors of n.

Find the following:
a. $S(1)$ **b.** $S(15)$ **c.** $S(17)$
d. $S(5)$ **e.** $S(18)$ **f.** $S(21)$

10. Let D be the set of all finite subsets of positive integers.

Define a function $T : \mathbf{Z}^+ \to D$ as follows: For each positive integer n, $T(n) =$ the set of positive divisors of n.

Find the following:
a. $T(1)$ **b.** $T(15)$ **c.** $T(17)$
d. $T(5)$ **e.** $T(18)$ **f.** $T(21)$

11. Define $F : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} \times \mathbf{Z}$ as follows: For every ordered pair (a, b) of integers, $F(a, b) = (2a + 1, 3b - 2)$.

Find the following:
a. $F(4, 4)$ **b.** $F(2, 1)$ **c.** $F(3, 2)$ **d.** $F(1, 5)$

12. Let $J_5 = \{0, 1, 2, 3, 4\}$, and define $G : J_5 \times J_5 \to J_5 \times J_5$ as follows: For each $(a, b) \in J_5 \times J_5$,

$$G(a, b) = ((2a + 1) \bmod 5, (3b - 2) \bmod 5).$$

Find the following:
a. $G(4, 4)$ **b.** $G(2, 1)$ **c.** $G(3, 2)$ **d.** $G(1, 5)$

13. Let $J_5 = \{0, 1, 2, 3, 4\}$, and define functions $f : J_5 \to J_5$ and $g : J_5 \to J_5$ as follows: For each $x \in J_5$,

$$f(x) = (x + 4)^2 \bmod 5 \text{ and}$$
$$g(x) = (x^2 + 3x + 1) \bmod 5.$$

Is $f = g$? Explain.

14. Define functions H and K from $\mathbf{R}$ to $\mathbf{R}$ by the following formulas:

For every $x \in \mathbf{R}$,

$$H(x) = \lfloor x \rfloor + 1 \quad \text{and} \quad K(x) = \lceil x \rceil.$$

Does $H = K$? Explain.

15. Let F and G be functions from the set of all real numbers to itself. Define the product functions $F \cdot G : \mathbf{R} \to \mathbf{R}$ and $G \cdot F : \mathbf{R} \to \mathbf{R}$ as follows: For every $x \in \mathbf{R}$,

$$(F \cdot G)(x) = F(x) \cdot G(x)$$
$$(G \cdot F)(x) = G(x) \cdot F(x).$$

Does $F \cdot G = G \cdot F$? Explain.

16. Let F and G be functions from the set of all real numbers to itself. Define new functions $F - G : \mathbf{R} \to \mathbf{R}$ and $G - F : \mathbf{R} \to \mathbf{R}$ as follows: For every $x \in \mathbf{R}$,

$$(F - G)(x) = F(x) - G(x)$$
$$(G - F)(x) = G(x) - F(x).$$

Does $F - G = G - F$? Explain.

17. Use the definition of logarithm to fill in the blanks below.

a. $\log_2 8 = 3$ because _____.
b. $\log_5 \left(\frac{1}{25}\right) = -2$ because _____.
c. $\log_4 4 = 1$ because _____.
d. $\log_3 (3^n) = n$ because _____.
e. $\log_4 1 = 0$ because _____.

18. Find exact values for each of the following quantities without using a calculator.

a. $\log_3 81$ **b.** $\log_2 1024$ **c.** $\log_3 \left(\frac{1}{27}\right)$
d. $\log_2 1$ **e.** $\log_{10} \left(\frac{1}{10}\right)$ **f.** $\log_3 3$
g. $\log_2 (2^k)$

19. Use the definition of logarithm to prove that for any positive real number b with $b \neq 1$, $\log_b b = 1$.

20. Use the definition of logarithm to prove that for any positive real number b with $b \neq 1$, $\log_b 1 = 0$.

21. If b is any positive real number with $b \neq 1$ and x is any real number, b^{-x} is defined as follows: $b^{-x} = \dfrac{1}{b^x}$. Use this definition and the definition of logarithm to prove that $\log_b \left(\dfrac{1}{u}\right) = -\log_b(u)$ for all positive real numbers u and b, with $b \neq 1$.

***H* 22.** Use the unique factorization for the integers theorem (Section 4.4) and the definition of logarithm to prove that $\log_3 (7)$ is irrational.

23. If b and y are positive real numbers such that $\log_b y = 3$, what is $\log_{1/b} (y)$? Explain.

24. If b and y are positive real numbers such that $\log_b y = 2$, what is $\log_{b^2}(y)$? Explain.

25. Let $A = \{2, 3, 5\}$ and $B = \{x, y\}$. Let p_1 and p_2 be the **projections of $A \times B$ onto the first and second coordinates**. That is, for each pair $(a, b) \in A \times B$, $p_1(a, b) = a$ and $p_2(a, b) = b$.

a. Find $p_1(2, y)$ and $p_1(5, x)$. What is the range of p_1?
b. Find $p_2(2, y)$ and $p_2(5, x)$. What is the range of p_2?

26. Observe that *mod* and *div* can be defined as functions from $\mathbf{Z}^{nonneg} \times \mathbf{Z}^+$ to $\mathbf{Z}$. For each ordered pair (n, d) consisting of a nonnegative integer n and a positive integer d, let

$mod(n, d) = n \bmod d$ (the nonnegative remainder obtained when n is divided by d).

$div(n, d) = n \operatorname{div} d$ (the integer quotient obtained when n is divided by d).

Find each of the following:

a. *mod* (67, 10) and *div* (67, 10)
b. *mod* (59, 8) and *div* (59, 8)
c. *mod* (30, 5) and *div* (30, 5)

27. Let S be the set of all strings of a's and b's.

a. Define $f : S \to Z$ as follows: For each string s in S

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left} \\ \text{of the left-most } a \text{ in } s \\ 0 \quad \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

b. Define $g : S \to S$ as follows: For each string s in S,

$g(s) =$ the string obtained by writing the characters of s in reverse order.

Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g?

28. Consider the coding and decoding functions E and D defined in Example 7.1.9.

a. Find $E(0110)$ and $D(111111000111)$.
b. Find $E(1010)$ and $D(000000111111)$.

29. Consider the Hamming distance function defined in Example 7.1.10.

a. Find $H(10101, 00011)$.
b. Find $H(00110, 10111)$.

30. Draw arrow diagrams for the Boolean functions defined by the following input/output tables.

a.

Input		Output
P	*Q*	*R*
1	1	0
1	0	1
0	1	0
0	0	1

b.

Input			Output
P	*Q*	*R*	*S*
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

31. Fill in the following table to show the values of all possible two-place Boolean functions.

Input		f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1																
1	0																
0	1																
0	0																

32. Consider the three-place Boolean function f defined by the following rule: For each triple (x_1, x_2, x_3) of 0's and 1's,

$$f(x_1, x_2, x_3) = (4x_1 + 3x_2 + 2x_3) \textit{ mod } 2.$$

a. Find $f(1, 1, 1)$ and $f(0, 0, 1)$.
b. Describe f using an input/output table.

33. Student A tries to define a function $g : \mathbf{Q} \to \mathbf{Z}$ by the rule

$$g\left(\frac{m}{n}\right) = m - n, \text{ for all integers } m \text{ and } n \text{ with } n \neq 0.$$

Student B claims that g is not well defined. Justify student B's claim.

34. Student C tries to define a function $h : \mathbf{Q} \to \mathbf{Q}$ by the rule

$$h\left(\frac{m}{n}\right) = \frac{m^2}{n}, \text{ for all integers } m \text{ and } n \text{ with } n \neq 0.$$

Student D claims that h is not well defined. Justify student D's claim.

35. Let $U = \{1, 2, 3, 4\}$. Student A tries to define a function $R : U \to Z$ as follows: For each $x \in U$,

$R(x)$ is the integer y so that (xy) *mod* $5 = 1$.

Student B claims that R is not well defined. Who is correct: student A or student B? Justify your answer.

36. Let $V = \{1, 2, 3\}$. Student C tries to define a function $S : V \to V$ as follows: For each $x \in V$,

$S(x)$ is the integer y in V so that (xy) *mod* $4 = 1$.

Student D claims that S is not well defined. Who is right: student C or student D? Justify your answer.

37. On certain computers the integer data type goes from −2,147,483,648 through 2,147,483,647. Let S be the set of all integers from −2,147,483,648 through 2,147,483,647. Try to define a function $f : S \to S$ by the rule $f(n) = n^2$ for each n in S. Is f well defined? Explain.

38. Let $X = \{a, b, c\}$ and $Y = \{r, s, t, u, v, w\}$. Define $f : X \to Y$ as follows: $f(a) = v$, $f(b) = v$, and $f(c) = t$.
a. Draw an arrow diagram for f.
b. Let $A = \{a, b\}$, $C = \{t\}$, $D = \{u, v\}$, and $E = \{r, s\}$. Find $f(A)$, $f(X)$, $f^{-1}(C)$, $f^{-1}(D)$, $f^{-1}(E)$, and $f^{-1}(Y)$.

39. Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$. Define $g : X \to Y$ as follows: $g(1) = a$, $g(2) = a$, $g(3) = a$, and $g(4) = d$.
a. Draw an arrow diagram for g.
b. Let $A = \{2, 3\}$, $C = \{a\}$, and $D = \{b, c\}$. Find $g(A)$, $g(X)$, $g^{-1}(C)$, $g^{-1}(D)$, and $g^{-1}(Y)$.

***H* 40.** Let X and Y be sets, let A and B be any subsets of X, and let F be a function from X to Y. Fill in the blanks in the following proof that $F(A) \cup F(B) \subseteq F(A \cup B)$.

Proof: Let y be any element in $F(A) \cup F(B)$. *[We must show that y is in $F(A \cup B)$.]* By definition of union, $\underline{\quad (i) \quad}$.

***Case 1*, $y \in F(A)$:** In this case, by definition of $F(A)$, $y = F(x)$ for $\underline{\quad (ii) \quad}$ $x \in A$. Since $A \subseteq A \cup B$,

it follows from the definition of union that $x \in$ ___(iii)___. Hence, $y = F(x)$ for some $x \in A \cup B$, and thus, by definition of $F(A \cup B)$, $y \in$ ___(iv)___.

***Case 2*, $y \in F(B)$:** In this case, by definition of $F(B)$, ___(v)___ for some $x \in B$. Since $B \subseteq A \cup B$ it follows from the definition of union that ___(vi)___. Thus $y \in F(A \cup B)$.

Therefore, regardless of whether $y \in F(A)$ or $y \in F(B)$, we have that $y \in F(A \cup B)$ *[as was to be shown]*.

In 41–49 let X and Y be sets, let A and B be any subsets of X, and let C and D be any subsets of Y. Determine which of the properties are true for every function F from X to Y and which are false for at least one function F from X to Y. Justify your answers.

41. If $A \subseteq B$ then $F(A) \subseteq F(B)$.

42. $F(A \cap B) \subseteq F(A) \cap F(B)$

43. $F(A) \cap F(B) \subseteq F(A \cap B)$

44. For all subsets A and B of X, $F(A - B) = F(A) - F(B)$.

45. For all subsets C and D of Y, if $C \subseteq D$, then

$$F^{-1}(C) \subseteq F^{-1}(D).$$

H 46. For all subsets C and D of Y,

$$F^{-1}(C \cup D) = F^{-1}(C) \cup F^{-1}(D).$$

47. For all subsets C and D of Y,

$$F^{-1}(C \cap D) = F^{-1}(C) \cap F^{-1}(D).$$

48. For all subsets C and D of Y,

$$F^{-1}(C - D) = F^{-1}(C) - F^{-1}(D).$$

49. $F(F^{-1}(C)) \subseteq C$

50. Given a set S and a subset A, the **characteristic function of A**, denoted χ_A, is the function defined from S to $\mathbf{Z}$ with the property that for each $u \in S$,

$$\chi_A(u) = \begin{cases} 1 & \text{if } u \in A \\ 0 & \text{if } u \notin A. \end{cases}$$

Show that each of the following holds for all subsets A and B of S and every $u \in S$.

a. $\chi_{A \cap B}(u) = \chi_A(u) \cdot \chi_B(u)$

b. $\chi_{A \cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$

Each of exercises 51–53 refers to the Euler phi function, denoted ϕ, which is defined as follows: For each integer $n \geq 1$, $\phi(n)$ is the number of positive integers less than or equal to n that have no common factors with n except ± 1. For example, $\phi(10) = 4$ because there are four positive integers less than or equal to 10 that have no common factors with 10 except ± 1—namely, 1, 3, 7, and 9.

51. Find each of the following:

a. $\phi(15)$ **b.** $\phi(2)$ **c.** $\phi(5)$

d. $\phi(12)$ **e.** $\phi(11)$ **f.** $\phi(1)$

52. Prove that if p is a prime number and n is an integer with $n \geq 1$, then $\phi(p^n) = p^n - p^{n-1}$.

H 53. Prove that there are infinitely many integers n for which $\phi(n)$ is a perfect square.

ANSWERS FOR TEST YOURSELF

1. the unique output element in Y that is related to x by f **2.** the value of f at x; the image of x under f; the output of f for the input x **3.** the set of all y in Y such that $f(x) = y$ **4.** an inverse image of y under f; a preimage of y **5.** $\{x \in X \mid f(x) = y\}$; the inverse image of y **6.** $f(x) = g(x)$ for every $x \in X$ **7.** the exponent to which b must be raised to obtain x (*Or:* the real number y such that $x = b^y$) **8.** $\{y \in Y \mid y = f(x)$ for some $x \in A\}$ (*Or:* $\{f(x) \mid x \in A\}$) **9.** $\{x \in X \mid f(x) \in C\}$

7.2 One-to-One, Onto, and Inverse Functions

Don't accept a statement just because it is printed. —Anna Pell Wheeler, 1883–1966

In this section we discuss two important properties that functions may satisfy: the property of being *one-to-one* and the property of being *onto*. Functions that satisfy both properties are called *one-to-one correspondences* or *one-to-one onto functions*. When a function is a one-to-one correspondence, the elements of its domain and co-domain match up perfectly,

and we can define an *inverse function* from the co-domain to the domain that "undoes" the action of the function.

One-to-One Functions

In Section 7.1 we noted that a function may send several elements of its domain to the same element of its co-domain. In terms of arrow diagrams, this means that two or more arrows that start in the domain can point to the same element in the co-domain. On the other hand, if no two arrows that start in the domain point to the same element of the co-domain then the function is called *one-to-one* or *injective*. For a one-to-one function, each element of the co-domain is the image of at most one element of the domain.

Definition

Let F be a function from a set X to a set Y. F is **one-to-one** (or **injective**) if, and only if, for all elements x_1 and x_2 in X,

$$\text{if } F(x_1) = F(x_2), \text{ then } x_1 = x_2,$$

or, equivalently,

$$\text{if } x_1 \neq x_2, \text{ then } F(x_1) \neq F(x_2).$$

Symbolically:

$$F: X \to Y \text{ is one-to-one} \Leftrightarrow \forall x_1, x_2 \in X, \text{ if } F(x_1) = F(x_2) \text{ then } x_1 = x_2.$$

To obtain a precise statement of what it means for a function *not* to be one-to-one, take the negation of one of the equivalent versions of the definition above. Thus:

A function $F: X \to Y$ is *not* one-to-one $\Leftrightarrow$ $\exists$ elements x_1 and x_2 in X with $F(x_1) = F(x_2)$ and $x_1 \neq x_2$.

In other words, if elements x_1 and x_2 can be found that have the same function value but are not equal, then F is not one-to-one.

In terms of arrow diagrams, a one-to-one function can be thought of as a function that separates points. That is, it takes distinct points of the domain to distinct points of the co-domain. A function that is not one-to-one fails to separate points. In other words, at least two points of the domain are taken to the same point of the co-domain. This distinction is illustrated in Figures 7.2.1(a) and 7.2.1(b).

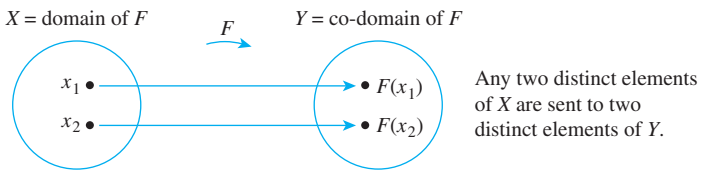


FIGURE 7.2.1(a) A One-to-One Function Separates Points

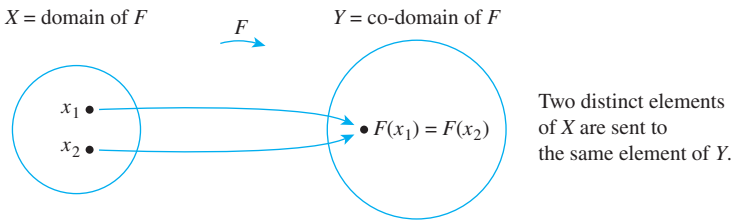


FIGURE 7.2.1(b) A Function That Is Not One-to-One Collapses Points Together

Example 7.2.1 **Identifying One-to-One Functions Defined on Finite Sets**

a. Do either of the arrow diagrams in Figure 7.2.2 define one-to-one functions?

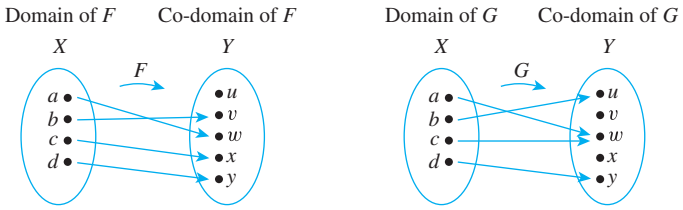


FIGURE 7.2.2

b. Let $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d\}$. Define $H: X \to Y$ as follows: $H(1) = c$, $H(2) = a$, and $H(3) = d$. Define $K: X \to Y$ as follows: $K(1) = d$, $K(2) = b$, and $K(3) = d$. Is either H or K one-to-one?

Solution

a. F is one-to-one but G is not. F is one-to-one because no two different elements of X are sent by F to the same element of Y. G is not one-to-one because the elements a and c are both sent by G to the same element of Y: $G(a) = G(c) = w$ but $a \neq c$.

b. H is one-to-one but K is not. H is one-to-one because each of the three elements of the domain of H is sent by H to a different element of the co-domain: $H(1) \neq H(2)$, $H(1) \neq H(3)$, and $H(2) \neq H(3)$. K, however, is not one-to-one because $K(1) = K(3) = d$ but $1 \neq 3$. ■

Consider the problem of writing a computer algorithm to check whether a function F is one-to-one. If F is defined on a finite set and there is an independent algorithm or a table of values for F, then an algorithm to check whether F is one-to-one can be written as follows: Represent the domain of F as a one-dimensional array $a[1]$, $a[2], \ldots, a[n]$ and use a nested loop to examine all possible pairs $(a[i], a[j])$, where $i < j$. If there is a pair $(a[i], a[j])$ for which $F(a[i]) = F(a[j])$ and $a[i] \neq a[j]$, then F is not one-to-one. If, however, all pairs have been examined without finding such a pair, then F is one-to-one. You are asked to write such an algorithm in exercise 57 at the end of this section.

One-to-One Functions on Infinite Sets

Now suppose f is a function defined on an infinite set X. By definition, f is one-to-one if, and only if, the following universal statement is true:

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$

Thus, to prove f is one-to-one, you will generally use the method of direct proof:

suppose x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$

and **show** that $x_1 = x_2$.

To show that f is *not* one-to-one, you will ordinarily

find elements x_1 and x_2 in X so that $f(x_1) = f(x_2)$ but $x_1 \neq x_2$.

Example 7.2.2 **Proving or Disproving That Functions Are One-to-One**

Define f: $\mathbf{R} \to \mathbf{R}$ and g: $\mathbf{Z} \to \mathbf{Z}$ by the rules

$$f(x) = 4x - 1 \quad \text{for all } x \in \mathbf{R}$$

and

$$g(n) = n^2 \quad \text{for all } n \in \mathbf{Z}.$$

a. Is f one-to-one? Prove or give a counterexample.

b. Is g one-to-one? Prove or give a counterexample.

Solution It is usually best to start by taking a positive approach to answering questions like these. Try to prove the given functions are one-to-one and see whether you run into difficulty. If you finish without running into any problems, then you have a proof. If you do encounter a problem, then analyzing the problem may lead you to discover a counterexample.

a. The function f: $\mathbf{R} \to \mathbf{R}$ is defined by the rule

$$f(x) = 4x - 1 \quad \text{for each real number } x.$$

To prove that f is one-to-one, you need to prove that

$$\forall \text{ real numbers } x_1 \text{ and } x_2, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$

Substituting the definition of f into the outline of a direct proof, you

suppose x_1 and x_2 are any real numbers such that $4x_1 - 1 = 4x_2 - 1$,

and **show** that $x_1 = x_2$.

Can you reach what is to be shown from the supposition? Yes. Just add 1 to both sides of the equation in the supposition and then divide both sides by 4.

This discussion is summarized in the following formal answer.

Answer to (a):

If the function f: $\mathbf{R} \to \mathbf{R}$ is defined by the rule $f(x) = 4x - 1$, for each real number x, then f is one-to-one.

Proof: Suppose x_1 and x_2 are real numbers such that $f(x_1) = f(x_2)$. *[We must show that $x_1 = x_2$.]* By definition of f,

$$4x_1 - 1 = 4x_2 - 1.$$

Adding 1 to both sides gives

$$4x_1 = 4x_2,$$

and dividing both sides by 4 gives

$$x_1 = x_2,$$

[as was to be shown].

b. The function g: $\mathbf{Z} \to \mathbf{Z}$ is defined by the rule

$$g(n) = n^2 \quad \text{for each integer } n.$$

As above, you start as though you were going to prove that g is one-to-one. Substituting the definition of g into the outline of a direct proof, you

suppose n_1 and n_2 are integers such that $n_1^2 = n_2^2$,

and **try to show** that $n_1 = n_2$.

Can you reach what is to be shown from the supposition? No! It is quite possible for two numbers to have the same squares and yet be different. For example, $2^2 = (-2)^2$ but $2 \neq -2$.

Thus, in trying to prove that g is one-to-one, you run into difficulty. But analyzing this difficulty leads to the discovery of a counterexample, which shows that g is not one-to-one.

This discussion is summarized as follows:

Answer to (b):

If the function g: $\mathbf{Z} \to \mathbf{Z}$ is defined by the rule $g(n) = n^2$, for all $n \in \mathbf{Z}$, then g is not one-to-one.

Counterexample:

Let $n_1 = 2$ and $n_2 = -2$. Then by definition of g,

$$g(n_1) = g(2) = 2^2 = 4 \text{ and also}$$
$$g(n_2) = g(-2) = (-2)^2 = 4.$$

Hence $g(n_1) = g(n_2)$ but $n_1 \neq n_2$,

and so g is not one-to-one.

■

Application: Hash Functions

Imagine a university with 10,000 students each with a nine-digit ID number, which the university plans to link to student records. Placing the record with ID number n in position n of an array would waste computer memory space because only a small fraction of the billion possible nine-digit ID numbers are needed for the 10,000 students.

Definition: Hash Function

A **hash function** is a function defined from a larger, possibly infinite, set of data to a smaller fixed-size set of integers.

To make it efficient for the university to store the records, a hash function is needed that (1) is one-to-one and (2) has a co-domain that is very much smaller than one billion. Most hash functions are modifications of *mod* functions and are defined using prime numbers to increase the chance that their values will be scattered rather than clustered together. In addition, making their co-domains 50% to 100% larger than their domains makes it more

likely that they will be one-to-one. Nonetheless, two input values may **collide**, that is, have the same output value, and various methods are used to avoid such a **collision**. One of these is illustrated in the following very much simplified example to address the university's situation.

Example 7.2.3 **Computing Values of a Hash Function**

Instead of 10,000 students, suppose there are only 6. Define a function H, from the set of student ID numbers to the set {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10} as follows:

$$H(n) = n \textit{ mod } 11 \text{ for each ID number } n.$$

To compute values of H either use a calculator or a computer with a built-in *mod* function or use the formula $n \textit{ mod } 11 = n - (n \textit{ div } 11)$ from Section 4.5. In other words, divide n by 11, multiply the integer part of the result by 11, and subtract that number from n. As an example, since 328343419/11 = 29849401.73.

$$H(328343419) = 328343419 - (11 \cdot 29849401) = 8$$

To store the link to the record for the student with ID number n, start by computing $H(n)$. For instance, if the ID numbers are 328343419, 356633102, 223799061, and 513408716, the corresponding H-values are as shown in Table 7.2.1.

TABLE 7.2.1

	0
356633102	1
223799061	2
	3
	4
	5
	6
513408716	7
328343419	8
	9
	10

As noted above, H may not be one-to-one: two different ID numbers could have the same H-value. But because it is important for each value in the table to link to a single student record, a **collision resolution** method is needed. One of the simplest, called a **linear probe**, works as follows: If $H(n)$ is already occupied when a new student ID number is input, start from $H(n)$ in the table and search downward to put a link for the student's record in the first empty position that occurs; if no empty positions remain going down, go up to the beginning of the table and search from there. Because 11 is greater than 6, empty positions are guaranteed.

Suppose the ID number for another student is 607275830. Find the position in the table for this number.

Solution When you compute $H(607275830)$ you find that it equals 7, which is already occupied by the link to the record for ID number 513408716. Searching downward from position 7, you find that position 8 is also occupied but position 9 is free.

$$607275830 \longrightarrow \underset{\text{occupied}}{7} \longrightarrow \underset{\text{occupied}}{8} \longrightarrow \underset{\text{free}}{9}$$

Therefore, you put the link for the record with ID number 607275830 in position 9. ■

A special class of hash functions, known as *cryptographic hash functions*, is used to secure digital data. A **cryptographic hash function** is designed to satisfy the following conditions:

1. It is a function from bit strings to bit strings of a fixed length.
2. It is close to being one-to-one: the probability of collisions is very small.
3. It is close to being a *one-way function*: given any bit string in its range, finding the inverse image of the string is computationally very difficult.
4. Its values can be quickly computed.
5. A very slight change in an input string results in an extensive change in the output string.

One use of cryptographic hash functions is to provide password security. Passwords in a company's user account file are almost never stored as "clear" text. A basic protection is to apply a cryptographic hash function to the passwords, or to a combination consisting of the passwords plus extra content provided by the company, and to store only the values of the hash function, called the *hashes*. To log in, a user keys in a password, which is immediately *hashed* (meaning that its value is input to the hash function), and the result is compared to the hash stored in the account file. In order to complete the login process, the two hashes have to agree.

A somewhat similar kind of hashing is used for checking the integrity of files. When a file is intended to be copied, a cryptographic hash function is applied to it. The accuracy of a copy is checked by applying the same hash function. If the two hashes agree, the copy is accepted. Similarly, when A needs to send a file through a possibly insecure network to B, A can first apply a cryptographic hash function to the file. Then A sends the hash separately to B through a secure network, and when B receives the file, B applies the same hash function to it that A used. B compares the result with the hash received from A, and if the two agree, B can have confidence that the file was unchanged during transmission.

Cryptographic hash functions are also used in *blockchain* technology. A blockchain is a public register on the Internet made up of linked blocks consisting of records or programs. To make it impossible to change the data in any part of a block, each includes a time stamp plus a hash computed from all the previous parts of the blockchain. To keep the system operating at a reasonable pace and to validate additions, a time-consuming *proof of work* is required to add a block to the blockchain. A commonly used proof of work requires a programmer to use repeated random trials, to discover the input that needs to be added to the data in the blockchain so that when the two are hashed together the output will contain a specified number of initial zeroes.

Onto Functions

It was noted in Section 7.1 that there may be an element of the co-domain of a function that is not the image of any element in the domain. On the other hand, it is possible for *every* element in a function's co-domain to be the image of some element in its domain.

Such a function is called *onto* or *surjective*. When a function is onto, its range is equal to its co-domain.

Definition

Let F be a function from a set X to a set Y. F is **onto** (or **surjective**) if, and only if, given any element y in Y, it is possible to find an element x in X with the property that $y = F(x)$.

Symbolically:

$$F: X \to Y \text{ is onto} \quad \Leftrightarrow \quad \forall y \in Y, \exists x \in X \text{ such that } F(x) = y.$$

To obtain a precise statement of what it means for a function *not* to be onto, take the negation of the definition of onto:

$$F: X \to Y \text{ is } \textit{not} \text{ onto} \quad \Leftrightarrow \quad \exists y \text{ in } Y \text{ such that } \forall x \in X, F(x) \neq y.$$

That is, there is some element in Y that is *not* the image of *any* element in X.

In terms of arrow diagrams, a function is onto if each element of the co-domain has an arrow pointing to it from some element of the domain. A function is not onto if at least one element in its co-domain does not have an arrow pointing to it. This is illustrated in Figures 7.2.3(a) and 7.2.3(b).

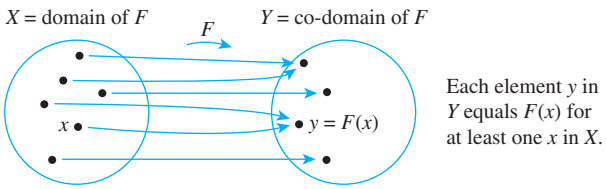


FIGURE 7.2.3(a) A Function That Is Onto

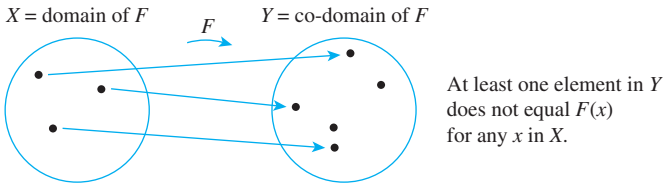


FIGURE 7.2.3(b) A Function That Is Not Onto

Example 7.2.4 **Identifying Onto Functions Defined on Finite Sets**

a. Do either of the arrow diagrams in Figure 7.2.4 define onto functions?

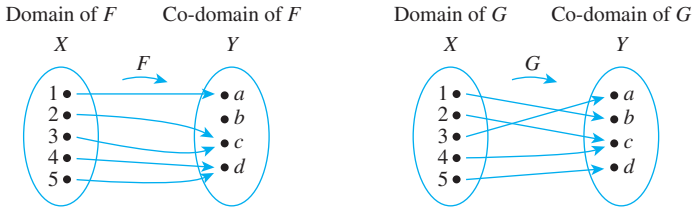


FIGURE 7.2.4

b. Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$. Define $H: X \to Y$ as follows: $H(1) = c$, $H(2) = a$, $H(3) = c$, $H(4) = b$. Define $K: X \to Y$ as follows: $K(1) = c$, $K(2) = b$, $K(3) = b$, and $K(4) = c$. Is either H or K onto?

Solution

a. F is not onto because $b \neq F(x)$ for any x in X. G is onto because each element of Y equals $G(x)$ for some x in X: $a = G(3)$, $b = G(1)$, $c = G(2) = G(4)$, and $d = G(5)$.

b. H is onto but K is not. H is onto because each of the three elements of the co-domain of H is the image of some element of the domain of H: $a = H(2)$, $b = H(4)$, and $c = H(1) = H(3)$. K, however, is not onto because $a \neq K(x)$ for any x in $\{1, 2, 3, 4\}$.

■

It is possible to write a computer algorithm to check whether a function F is onto, provided F is defined from a finite set X to a finite set Y and there is an independent algorithm or table of values for F. Represent X and Y as one-dimensional arrays $a[1], a[2], \ldots, a[n]$ and $b[1], b[2], \ldots, b[m]$, respectively. Use a nested loop to pick each element y of Y in turn, and search through the elements of X to find an x such that y is the image of x. If any search is unsuccessful, then F is not onto. If each such search is successful, then F is onto. You are asked to write such an algorithm in exercise 58 at the end of this section.

Onto Functions on Infinite Sets

Now suppose F is a function from a set X to a set Y, and suppose Y is infinite. By definition, F is onto if, and only if, the following universal statement is true:

$$\forall y \in Y, \exists x \in X \text{ such that } F(x) = y.$$

Thus to prove F is onto, you will ordinarily use the method of generalizing from the generic particular:

suppose that y is any element of Y

and **show** that there is an element x in X with $F(x) = y$.

To prove F is *not* onto, you will usually

find an element y of Y such that $y \neq F(x)$ for *any* x in X.

Example 7.2.5 **Proving or Disproving That Functions Are Onto**

Define $f: \mathbf{R} \to \mathbf{R}$ and $h: \mathbf{Z} \to \mathbf{Z}$ by the rules

$$f(x) = 4x - 1 \text{ for each } x \in \mathbf{R}$$

and

$$h(n) = 4n - 1 \text{ for each } n \in \mathbf{Z}.$$

a. Is f onto? Prove or give a counterexample.

b. Is h onto? Prove or give a counterexample.

Solution

a. The best approach is to start trying to prove that f is onto and be alert for difficulties that might indicate that it is not. Now $f: \mathbf{R} \to \mathbf{R}$ is the function defined by the rule

$$f(x) = 4x - 1 \quad \text{for each real number } x.$$

To prove that f is onto, you must prove

$$\forall y \in Y, \exists x \in X \text{ such that } f(x) = y.$$

Substituting the definition of f into the outline of a proof by the method of generalizing from the generic particular, you

suppose y is a real number

and **show** that there exists a real number x such that $y = 4x - 1$.

Caution! This scratch work only proves what x has to be *if* it exists. The scratch work does not prove that x exists.

Scratch Work: **If** such a real number x exists, then

$$\begin{aligned} 4x - 1 &= y \\ 4x &= y + 1 && \text{by adding 1 to both sides} \\ x &= \frac{y+1}{4} && \text{by dividing both sides by 4.} \end{aligned}$$

Thus *if* such a number x exists, it must equal $(y + 1)/4$. Does such a number exist? Yes. To show this, let $x = (y + 1)/4$, and then make sure that (1) x is a real number and that (2) f really does send x to y. The following formal answer summarizes this process.

Answer to (a):

If $f: \mathbf{R} \to \mathbf{R}$ is the function defined by the rule $f(x) = 4x - 1$ for each real number x, then f is onto.

Proof: Let $y \in \mathbf{R}$. *[We must show that $\exists x$ in $\mathbf{R}$ such that $f(x) = y$.]* Let $x = (y + 1)/4$. Then x is a real number since sums and quotients (other than by 0) of real numbers are real numbers. It follows that

$$\begin{aligned} f(x) &= f\left(\frac{y+1}{4}\right) && \text{by substitution} \\ &= 4 \cdot \left(\frac{y+1}{4}\right) - 1 && \text{by definition of } f \\ &= (y + 1) - 1 = y && \text{by basic algebra,} \end{aligned}$$

[as was to be shown].

b. The function $h: \mathbf{Z} \to \mathbf{Z}$ is defined by the rule

$$h(n) = 4n - 1 \quad \text{for each integer } n.$$

To prove that h is onto, you must prove that

$$\forall \text{ integer } m, \exists \text{ an integer } n \text{ such that } h(n) = m.$$

Substituting the definition of h into the outline of a proof by the method of generalizing from the generic particular shows that you need to

suppose m is any integer

and **show** that there is an integer n with $4n - 1 = m$.

Can you reach what is to be shown from the supposition? No! If $4n - 1 = m$,

$$n = \frac{m+1}{4} \quad \text{by adding 1 and dividing by 4.}$$

But n must be an integer. And when, for example, $m = 0$,

$$n = \frac{0+1}{4} = \frac{1}{4},$$

which is *not* an integer.

Thus, in trying to prove that h is onto, you run into difficulty, and this difficulty reveals a counterexample that shows h is not onto.

This discussion is summarized in the following formal answer.

Answer to (b):

If the function $h: \mathbf{Z} \to \mathbf{Z}$ is defined by the rule $h(n) = 4n - 1$ for each integer n, then h is not onto.

Counterexample: The co-domain of h is $\mathbf{Z}$ and $0 \in \mathbf{Z}$. But $h(n) \neq 0$ for any integer n. For if $h(n) = 0$, then

$$4n - 1 = 0 \quad \text{by definition of } h$$

which implies that

$$4n = 1 \quad \text{by adding 1 to both sides}$$

and so

$$n = \frac{1}{4} \quad \text{by dividing both sides by 4.}$$

But $\frac{1}{4}$ is not an integer. Hence there is no integer n for which $f(n) = 0$, and thus f is not onto.

■

Relations between Exponential and Logarithmic Functions

Note That the quantity b^x is a real number for any real number x follows from the least-upper-bound property of the real number system. (See Appendix A.)

For positive numbers $b \neq 1$, the **exponential function with base b**, denoted $\exp_b$, is the function from $\mathbf{R}$ to $\mathbf{R}^+$ defined as follows: For each real number x,

$$\exp_b(x) = b^x,$$

where $b^0 = 1$ and $b^{-x} = 1/b^x$.

When working with the exponential function, it is useful to recall the laws of exponents from elementary algebra.

Laws of Exponents

If b and c are any positive real numbers and u and v are any real numbers, the following laws of exponents hold true:

$$b^u b^v = b^{u+v} \tag{7.2.1}$$

$$(b^u)^v = b^{uv} \tag{7.2.2}$$

$$\frac{b^u}{b^u} = b^{u-v} \tag{7.2.3}$$

$$(bc)^u = b^u c^u \tag{7.2.4}$$

In Section 7.1 the logarithmic function with base b was defined for any positive number $b \neq 1$ to be the function from $\mathbf{R}^+$ to $\mathbf{R}$ with the property that for each positive real number x,

$$\log_b(x) = \text{the exponent to which } b \text{ must be raised to obtain } x.$$

Or, equivalently, for each positive real number x and real number y,

$$\log_b x = y \quad \Leftrightarrow \quad b^y = x.$$

It can be shown using calculus that both the exponential and logarithmic functions are one-to-one and onto. Therefore, by definition of one-to-one, the following properties hold true:

For any positive real number b with $b \neq 1$,

$$\text{if } b^u = b^v \text{ then } u = v \text{ for all real numbers } u \text{ and } v, \qquad 7.2.5$$

and

$$\text{if } \log_b u = \log_b v \text{ then } u = v \text{ for all positive real numbers } u \text{ and } v. \qquad 7.2.6$$

These properties are used to derive many additional facts about exponents and logarithms. In particular we have the following properties of logarithms.

Theorem 7.2.1 Properties of Logarithms

For any positive real numbers b, c, x, and y with $b \neq 1$ and $c \neq 1$ and for every real number a:

a. $\log_b(xy) = \log_b x + \log_b y$

b. $\log_b\left(\dfrac{x}{y}\right) = \log_b x - \log_b y$

c. $\log_b(x^a) = a \log_b x$

d. $\log_c x = \dfrac{\log_b x}{\log_b c}$

Theorem 7.2.1(d) is proved in the next example. You are asked to prove the remainder of the theorem in exercises 33–35 at the end of this section.

Example 7.2.6 **Using the One-to-Oneness of the Exponential Function**

Use the definition of logarithm, the laws of exponents, and the one-to-oneness of the exponential function (property 7.2.5) to prove part (d) of Theorem 7.2.1: For any positive real numbers b, c, and x, with $b \neq 1$ and $c \neq 1$,

$$\log_c x = \frac{\log_b x}{\log_b c}.$$

Solution Suppose positive real numbers b, c, and x are given with $b \neq 1$ and $c \neq 1$. Let

(1) $u = \log_b c$ (2) $v = \log_c x$ (3) $w = \log_b x$.

Then, by definition of logarithm,

$$(1')\ c = b^u \qquad (2')\ x = c^v \qquad (3')\ x = b^w.$$

Substituting (1′) into (2′) and using one of the laws of exponents gives

$$x = c^v = (b^u)^v = b^{uv} \quad \text{by 7.2.2.}$$

Now by (3), $x = b^w$ also. Hence

$$b^{uv} = b^w,$$

and so by the one-to-oneness of the exponential function (property 7.2.5),

$$uv = w.$$

Substituting from (1), (2), and (3) gives that

$$(\log_b c)(\log_c x) = \log_b x.$$

And dividing both sides by $\log_b c$ (which is nonzero because $c \neq 1$) results in

$$\log_c x = \frac{\log_b x}{\log_b c}.$$ ■

Example 7.2.7 **Computing Logarithms with Base 2 on a Calculator**

In computer science it is often necessary to compute logarithms with base 2. Most calculators do not have keys to compute logarithms with base 2 but do have keys to compute logarithms with base 10 (called **common logarithms** and often denoted simply log) and logarithms with base e (called **natural logarithms** and usually denoted ln). Suppose your calculator shows that $\ln 5 \approx 1.609437912$ and $\ln 2 \approx 0.6931471806$. Use Theorem 7.2.1(d) to find an approximate value for $\log_2 5$.

Solution By Theorem 7.2.1(d),

$$\log_2 5 = \frac{\ln 5}{\ln 2} \approx \frac{1.609437912}{0.6931471806} \approx 2.321928095.$$ ■

One-to-One Correspondences

Consider a function $F: X \to Y$ that is both one-to-one and onto. Given any element x in X, there is a unique corresponding element $y = F(x)$ in Y (since F is a function). Also given any element y in Y, there is an element x in X such that $F(x) = y$ (since F is onto) and there is only one such x (since F is one-to-one). Thus, a function that is one-to-one and onto sets up a pairing between the elements of X and the elements of Y that matches each element of X with exactly one element of Y and each element of Y with exactly one element of X. Such a pairing is called a *one-to-one correspondence* or *bijection* and is illustrated by the arrow diagram in Figure 7.2.5. One-to-one correspondences are often used as aids to counting. The pairing of Figure 7.2.5, for example, shows that there are five elements in the set X.

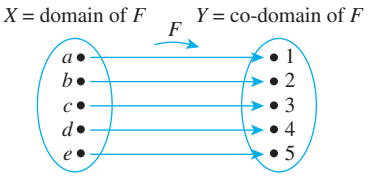


FIGURE 7.2.5 An Arrow Diagram for a One-to-One Correspondence

Definition

A **one-to-one correspondence** (or **bijection**) from a set X to a set Y is a function $F: X \to Y$ that is both one-to-one and onto.

Example 7.2.8 **A Function from a Power Set to a Set of Strings**

Let $\mathcal{P}(\{a, b\})$ be the set of all subsets of $\{a, b\}$ and let S be the set of all strings of length 2 made up of 0's and 1's. Then $\mathcal{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$ and $S = \{00, 01, 10, 11\}$. Define a function h from $\mathcal{P}(\{a, b\})$ to S as follows: Given any subset A of $\{a, b\}$, a is either in A or not in A, and b is either in A or not in A. If a is in A, write a 1 in the first position of the string $h(A)$; otherwise write a 0 there. Similarly, if b is in A, write a 1 in the second position of the string $h(A)$; otherwise write a 0 there. This definition is summarized in the following table.

h

Subset A of $\{a, b\}$	Status of a in A	Status of b in A	String $h(A)$ in S
$\varnothing$	not in	not in	00
$\{a\}$	in	not in	10
$\{b\}$	not in	in	01
$\{a, b\}$	in	in	11

Is h a one-to-one correspondence?

Solution The arrow diagram shown in Figure 7.2.6 shows clearly that h is a one-to-one correspondence. It is onto because each element of S has an arrow pointing to it. It is one-to-one because each element of S has no more than one arrow pointing to it.

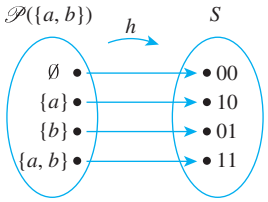


FIGURE 7.2.6

■

Example 7.2.9 **A String-Reversing Function**

Let T be the set of all finite strings of x's and y's. Define $g: T \to T$ by the following rule: For each string $s \in T$,

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Is g a one-to-one correspondence from T to itself?

Solution The answer is yes. To show that g is a one-to-one correspondence, it is necessary to show that g is one-to-one and onto.

To see that g is one-to-one, suppose that for some strings s_1 and s_2 in T, $g(s_1) = g(s_2)$. *[We must show that $s_1 = s_2$.]* Now to say that $g(s_1) = g(s_2)$ is the same as saying that the string

obtained by writing the characters of s_1 in reverse order equals the string obtained by writing the characters of s_2 in reverse order. But if s_1 and s_2 are equal when written in reverse order, then they must be equal to start with. In other words, $s_1 = s_2$ *[as was to be shown].*

To show that g is onto, suppose t is any string in T. *[We must find a string s in T such that $g(s) = t$.]* Let $s = g(t)$. By definition of g, $s = g(t)$ is the string in T obtained by writing the characters of t in reverse order. But when the order of the characters of a string is reversed once and then reversed again, the original string is recovered. Thus

$$\begin{aligned} g(s) = g(g(t)) &= \text{the string obtained by writing the characters} \\ &\quad \text{of } t \text{ in reverse order and then writing those} \\ &\quad \text{characters in reverse order again} \\ &= t, \end{aligned}$$

[as was to be shown]. ■

Example 7.2.10 **A Function of Two Variables**

Define a function $F: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: For every $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$F(x, y) = (x + y, x - y).$$

Is F a one-to-one correspondence from $\mathbf{R} \times \mathbf{R}$ to itself?

Solution The answer is yes. Showing that F is a one-to-one correspondence requires showing both that F is one-to-one and that F is onto.

Proof that F is one-to-one: Suppose that (x_1, y_1) and (x_2, y_2) are any ordered pairs in $\mathbf{R} \times \mathbf{R}$ such that

$$F(x_1, y_1) = F(x_2, y_2).$$

[We must show that $(x_1, y_1) = (x_2, y_2)$.] By definition of F,

$$(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2).$$

For two ordered pairs to be equal, both the first and second components must be equal. Thus x_1, y_1, x_2, and y_2 satisfy the following system of equations:

$$x_1 + y_1 = x_2 + y_2 \quad (1)$$
$$x_1 - y_1 = x_2 - y_2. \quad (2)$$

Adding equations (1) and (2) gives that

$$2x_1 = 2x_2, \quad \text{and so} \quad x_1 = x_2.$$

Substituting $x_1 = x_2$ into equation (1) yields

$$x_1 + y_1 = x_1 + y_2, \quad \text{and so} \quad y_1 = y_2.$$

Thus, by definition of equality of ordered pairs, $(x_1, y_1) = (x_2, y_2)$ *[as was to be shown].*

Caution! This scratch work only shows what (r, s) has to be *if* it exists. The scratch work does not prove that (r, s) exists.

Scratch work for the proof that F is onto: To prove that F is onto, suppose that you have any ordered pair—say (u, v)—in the co-domain $\mathbf{R} \times \mathbf{R}$ and then show that there is an ordered pair in the domain that is sent to (u, v) by F. To do this, suppose provisionally that you have found such an ordered pair, say (r, s). Then, on the one hand,

$$F(r, s) = (u, v) \qquad \text{because you are supposing that } F \text{ sends } (r, s) \text{ to } (u, v)$$

and, on the other hand,

$$F(r, s) = (r + s, r - s) \quad \text{by definition of } F.$$

Equating the right-hand sides of these two equations gives

$$(r + s, r - s) = (u, v).$$

By definition of equality of ordered pairs this means that

$$r + s = u \tag{1}$$
$$r - s = v. \tag{2}$$

To solve for r and s in terms of u and v, first add equations (1) and (2) to get

$$2r = u + v, \quad \text{and so} \quad r = \frac{u + v}{2}.$$

Then subtract equation (2) from equation (1) to obtain

$$2s = u - v, \quad \text{and so} \quad s = \frac{u - v}{2}.$$

Thus, ***if*** F sends (r, s) to (u, v), then $r = \frac{(u + v)}{2}$ and $s = \frac{(u - v)}{2}$. To turn this scratch work into a proof, you need to make sure that (1) $\left(\frac{u + v}{2}, \frac{u - v}{2}\right)$ is in the domain of F, and (2) that F really does send $\left(\frac{u + v}{2}, \frac{u - v}{2}\right)$ to (u, v).

Proof that F is onto: Suppose (u, v) is any ordered pair in the co-domain of F. *[We will show that there is an ordered pair in the domain of F that is sent to* (u, v) *by F.]* Let

$$r = \frac{u + v}{2} \quad \text{and} \quad s = \frac{u - v}{2}.$$

Then (r, s) is an ordered pair of real numbers, and so it is in the domain of F. In addition:

$$\begin{aligned}
F(r, s) &= F\left(\frac{u + v}{2}, \frac{u - v}{2}\right) && \text{by substitution} \\
&= \left(\frac{u + v}{2} + \frac{u - v}{2}, \frac{u + v}{2} - \frac{u - v}{2}\right) && \text{by definition of } F \\
&= \left(\frac{u + v + u - v}{2}, \frac{u + v - u + v}{2}\right) \\
&= \left(\frac{2u}{2}, \frac{2v}{2}\right) \\
&= (u, v) && \text{by algebra}
\end{aligned}$$

[as was to be shown]. ■

Inverse Functions

If F is a one-to-one correspondence from a set X to a set Y, then there is a function from Y to X that "undoes" the action of F; that is, it sends each element of Y back to the element of X that it came from. This function is called the *inverse function* for F.

Theorem 7.2.2

Suppose $F: X \to Y$ is a one-to-one correspondence; in other words, suppose F is one-to-one and onto. Then there is a function $\boldsymbol{F^{-1}: Y \to X}$ that is defined as follows: Given any element y in Y,

$$\boldsymbol{F^{-1}(y)} = \text{that unique element } x \text{ in } X \text{ such that } F(x) \text{ equals } y.$$

Or, equivalently,

$$F^{-1}(y) = x \quad \Leftrightarrow \quad y = F(x).$$

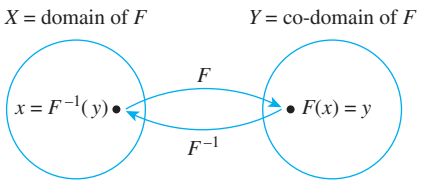
The proof of Theorem 7.2.2 follows immediately from the definition of one-to-one and onto. Given any element y in Y, there is an element x in X with $F(x) = y$ because F is onto; x is unique because F is one-to-one.

Definition

The function F^{-1} of Theorem 7.2.2 is called the **inverse function** for F.

Note that according to this definition, the logarithmic function with base $b > 0$ and $b \neq 1$ is the inverse of the exponential function with base b.

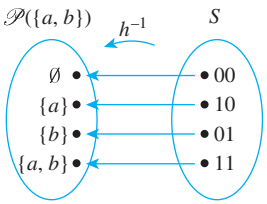
The diagram that follows illustrates the fact that an inverse function sends each element back to where it came from.



Example 7.2.11 **Finding an Inverse Function for a Function Given by an Arrow Diagram**

Define the inverse function for the one-to-one correspondence h given in Example 7.2.8.

Solution The arrow diagram for h^{-1} is obtained by tracing the h-arrows back from S to $\mathcal{P}(\{a, b\})$ as shown below.



$h^{-1}(00) = \emptyset \quad h^{-1}(10) = \{a\}$
$h^{-1}(01) = \{b\} \quad h^{-1}(11) = \{a, b\}$

■

Example 7.2.12 **Finding an Inverse Function for a Function Given in Words**

Define the inverse function for the one-to-one correspondence g given in Example 7.2.9.

Solution The function $g: T \to T$ is defined by the following rule:
For all strings t in T,

$$g(t) = \text{the string obtained by writing the characters of } t \text{ in reverse order.}$$

Now if the characters of t are written in reverse order and then written in reverse order again, the original string is recovered. Thus given any string t in T,

$$\begin{aligned} g^{-1}(t) &= \text{the unique string that, when written in reverse order, equals } t \\ &= \text{the string obtained by writing the characters of } t \text{ in reverse order} \\ &= g(t). \end{aligned}$$

Hence $g^{-1}: T \to T$ is the same as g, or, in other words, $g^{-1} = g$. ■

Example 7.2.13 **Finding an Inverse Function for a Function Given by a Formula**

The function $f: \mathbf{R} \to \mathbf{R}$ defined by the formula

$$f(x) = 4x - 1 \quad \text{for each real number } x$$

was shown to be one-to-one in Example 7.2.2 and onto in Example 7.2.5. Find its inverse function.

Solution For any *[particular but arbitrarily chosen]* y in $\mathbf{R}$, by definition of f^{-1},

$$f^{-1}(y) = \text{that unique real number } x \text{ such that } f(x) = y.$$

But

$$\begin{aligned} & f(x) = y \\ \Leftrightarrow \quad & 4x - 1 = y && \text{by definition of } f \\ \Leftrightarrow \quad & x = \frac{y+1}{4} && \text{by algebra.} \end{aligned}$$

Hence $f^{-1}(y) = \frac{y+1}{4}$. ■

The following theorem follows easily from the definitions.

Theorem 7.2.3

If X and Y are sets and $F: X \to Y$ is one-to-one and onto, then $F^{-1}: Y \to X$ is also one-to-one and onto.

Proof: ***F^{-1} is one-to-one:*** Suppose y_1 and y_2 are elements of Y such that $F^{-1}(y_1) = F^{-1}(y_2)$. *[We must show that $y_1 = y_2$.]* Let $x = F^{-1}(y_1) = F^{-1}(y_2)$. Then $x \in X$, and by definition of F^{-1},

$$F(x) = y_1 \quad \text{since } x = F^{-1}(y_1)$$

and

$$F(x) = y_2 \quad \text{since } x = F^{-1}(y_2).$$

Consequently, $y_1 = y_2$ because each is equal to $F(x)$. *[This is what was to be shown.]*

F^{-1} is onto: Suppose $x \in X$. *[We must show that there exists an element y in Y such that $F^{-1}(y) = x$.]* Let $y = F(x)$. Then $y \in Y$, and by definition of F^{-1}, $F^{-1}(y) = x$ *[as was to be shown].*

Example 7.2.14 **Finding an Inverse Function for a Function of Two Variables**

Define the inverse function F^{-1}: $\mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ for the one-to-one correspondence given in Example 7.2.10.

Solution The solution to Example 7.2.10 shows that $F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) = (u, v)$. Because F is one-to-one, this means that

$\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ is the unique ordered pair in the domain of F that is sent to (u, v) by F.

Thus, F^{-1} is defined as follows: For each ordered pair $(u, v) \in \mathbf{R} \times \mathbf{R}$,

$$F^{-1}(u, v) = \left(\frac{u+v}{2}, \frac{u-v}{2}\right).$$

■

TEST YOURSELF

1. If F is a function from a set X to a set Y, then F is one-to-one if, and only if, _____.
2. If F is a function from a set X to a set Y, then F is not one-to-one if, and only if, _____.
3. If F is a function from a set X to a set Y, then F is onto if, and only if, _____.
4. If F is a function from a set X to a set Y, then F is not onto if, and only if, _____.
5. The following two statements are _____:

   $\forall u, v \in U$, if $H(u) = H(v)$ then $u = v$.

   $\forall u, v \in U$, if $u \neq v$ then $H(u) \neq H(v)$.
6. Given a function $F: X \to Y$ where X is an infinite set, to prove that F is one-to-one, you suppose that _____ and then you show that _____.
7. Given a function $F: X \to Y$ where X is an infinite set, to prove that F is onto, you suppose that _____ and then you show that _____.
8. Given a function $F: X \to Y$, to prove that F is not one-to-one, you _____.
9. Given a function $F: X \to Y$, to prove that F is not onto, you _____.
10. A one-to-one correspondence from a set X to a set Y is a _____ that is _____.
11. If F is a one-to-one correspondence from a set X to a set Y and y is in Y, then $F^{-1}(y)$ is _____.

EXERCISE SET 7.2

1. The definition of one-to-one is stated in two ways:

   $\forall x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 = x_2$

   and $\forall x_1, x_2 \in X$, if $x_1 \neq x_2$ then $F(x_1) \neq F(x_2)$.

   Why are these two statements logically equivalent?

2. Fill in each blank with the word *most* or *least*.
   a. A function F is one-to-one if, and only if, each element in the co-domain of F is the image of at _____ one element in the domain of F.
   b. A function F is onto if, and only if, each element in the co-domain of F is the image of at _____ one element in the domain of F.

H 3. When asked to state the definition of one-to-one, a student replies, "A function f is one-to-one if, and only if, every element of X is sent by f to exactly one element of Y." Give a counterexample to show that the student's reply is incorrect.

H 4. Let $f: X \to Y$ be a function. True or false? A sufficient condition for f to be one-to-one is that for every element y in Y, there is at most one x in X with $f(x) = y$. Explain your answer.

H 5. All but two of the following statements are correct ways to express the fact that a function f is onto. Find the two that are incorrect.
   a. f is onto $\Leftrightarrow$ every element in its co-domain is the image of some element in its domain.
   b. f is onto $\Leftrightarrow$ every element in its domain has a corresponding image in its co-domain.
   c. f is onto $\Leftrightarrow$ $\forall y \in Y, \exists x \in X$ such that $f(x) = y$.

d. f is onto $\Leftrightarrow$ $\forall x \in X, \exists y \in Y$ such that $f(x) = y$.
e. f is onto $\Leftrightarrow$ the range of f is the same as the co-domain of f.

6. Let $X = \{1, 5, 9\}$ and $Y = \{3, 4, 7\}$.
a. Define $f: X \to Y$ by specifying that

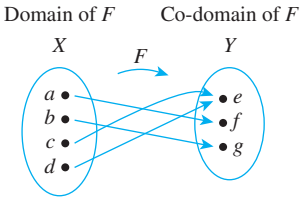
$$f(1) = 4, \quad f(5) = 7, \quad f(9) = 4.$$

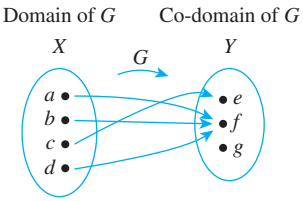
Is f one-to-one? Is f onto? Explain your answers.
b. Define $g: X \to Y$ by specifying that

$$g(1) = 7, \quad g(5) = 3, \quad g(9) = 4.$$

Is g one-to-one? Is g onto? Explain your answers.

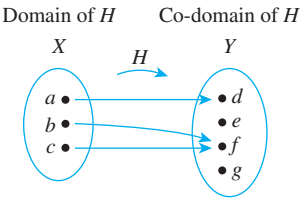
7. Let $X = \{a, b, c, d\}$ and $Y = \{e, f, g\}$. Define functions F and G by the arrow diagrams below.

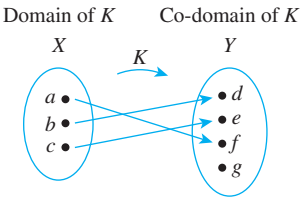




a. Is F one-to-one? Why or why not? Is it onto? Why or why not?
b. Is G one-to-one? Why or why not? Is it onto? Why or why not?

8. Let $X = \{a, b, c\}$ and $Y = \{d, e, f, g\}$. Define functions H and K by the arrow diagrams below.





a. Is H one-to-one? Why or why not? Is it onto? Why or why not?
b. Is K one-to-one? Why or why not? Is it onto? Why or why not?

9. Let $X = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$, and $Z = \{1, 2\}$.
a. Define a function $f: X \to Y$ that is one-to-one but not onto.
b. Define a function $g: X \to Z$ that is onto but not one-to-one.
c. Define a function $h: X \to X$ that is neither one-to-one nor onto.
d. Define a function $k: X \to X$ that is one-to-one and onto but is not the identity function on X.

10. **a.** Define $f: \mathbf{Z} \to \mathbf{Z}$ by the rule $f(n) = 2n$, for every integer n.
(i) Is f one-to-one? Prove or give a counterexample.
(ii) Is f onto? Prove or give a counterexample.
b. Let $2\mathbf{Z}$ denote the set of all even integers. That is, $2\mathbf{Z} = \{n \in \mathbf{Z} \mid n = 2k, \text{ for some integer } k\}$. Define $h: \mathbf{Z} \to 2\mathbf{Z}$ by the rule $h(n) = 2n$, for each integer n. Is h onto? Prove or give a counterexample.

***H* 11.** **a.** Define $g: \mathbf{Z} \to \mathbf{Z}$ by the rule $g(n) = 4n - 5$, for each integer n.
(i) Is g one-to-one? Prove or give a counterexample.
(ii) Is g onto? Prove or give a counterexample.
b. Define $G: \mathbf{R} \to \mathbf{R}$ by the rule $G(x) = 4x - 5$ for every real number x. Is G onto? Prove or give a counterexample.

12. **a.** Define $F: \mathbf{Z} \to \mathbf{Z}$ by the rule $F(n) = 2 - 3n$, for each integer n.
(i) Is F one-to-one? Prove or give a counterexample.
(ii) Is F onto? Prove or give a counterexample.
b. Define $G: \mathbf{R} \to \mathbf{R}$ by the rule $G(x) = 2 - 3x$ for each real number x. Is G onto? Prove or give a counterexample.

13. **a.** Define $H: \mathbf{R} \to \mathbf{R}$ by the rule $H(x) = x^2$, for each real number x.
(i) Is H one-to-one? Prove or give a counterexample.
(ii) Is H onto? Prove or give a counterexample.
b. Define $K: \mathbf{R}^{nonneg} \to \mathbf{R}^{nonneg}$ by the rule $K(x) = x^2$, for each nonnegative real number x. Is K onto? Prove or give a counterexample.

14. Explain the mistake in the following "proof."
Theorem: The function $f: \mathbf{Z} \to \mathbf{Z}$ defined by the formula $f(n) = 4n + 3$, for each integer n, is one-to-one.
"**Proof:** Suppose any integer n is given. Then by definition of f, there is only one possible value for $f(n)$—namely, $4n + 3$. Hence f is one-to-one."

In each of 15–18 a function f is defined on a set of real numbers. Determine whether or not f is one-to-one and justify your answer.

15. $f(x) = \dfrac{x+1}{x}$, for each number $x \neq 0$

16. $f(x) = \dfrac{x}{x^2+1}$, for each real number x

17. $f(x) = \dfrac{3x-1}{x}$, for each real number $x \neq 0$

18. $f(x) = \dfrac{x+1}{x-1}$, for each real number $x \neq 1$

19. Referring to Example 7.2.3, assume that records with the following ID numbers are to be placed in sequence into Table 7.2.1. Find the position into which each record is placed.
a. 417302072
b. 364981703
c. 283090787

20. Define Floor: $\mathbf{R} \to \mathbf{Z}$ by the formula $\text{Floor}(x) = \lfloor x \rfloor$, for every real number x.
a. Is Floor one-to-one? Prove or give a counterexample.
b. Is Floor onto? Prove or give a counterexample.

21. Let S be the set of all strings of 0's and 1's, and define $L: S \to Z^{nonneg}$ by

$$L(s) = \text{the length of } s, \quad \text{for every string } s \text{ in } S.$$

a. Is L one-to-one? Prove or give a counterexample.
b. Is L onto? Prove or give a counterexample.

22. Let S be the set of all strings of 0's and 1's, and define $D: S \to \mathbf{Z}$ as follows: For every $s \in S$,

$$D(s) = \text{the number of 1's in } s \text{ minus the number of 0's in } s.$$

a. Is D one-to-one? Prove or give a counterexample.
b. Is D onto? Prove or give a counterexample.

23. Define $F: \mathcal{P}(\{a, b, c\}) \to \mathbf{Z}$ as follows: For every A in $\mathcal{P}(\{a, b, c\})$,

$$F(A) = \text{the number of elements in } A.$$

a. Is F one-to-one? Prove or give a counterexample.
b. Is F onto? Prove or give a counterexample.

24. Les S be the set of all strings of a's and b's, and define $N: S \to \mathbf{Z}$ by

$$N(s) = \text{the number of } a\text{'s in } s, \quad \text{for each } s \in S.$$

a. Is N one-to-one? Prove or give a counterexample.
b. Is N onto? Prove or give a counterexample.

25. Let S be the set of all strings in a's and b's, and define $C: S \to S$ by

$$C(s) = as, \quad \text{for each } s \in S.$$

(C is called **concatenation** by a on the left.)
a. Is C one-to-one? Prove or give a counterexample.
b. Is C onto? Prove or give a counterexample.

26. Define $S: \mathbf{Z}^+ \to \mathbf{Z}^+$ by the rule: For each integer n, $S(n) =$ the sum of the positive divisors of n.
a. Is S one-to-one? Prove or give a counterexample.
b. Is S onto? Prove or give a counterexample.

***H* 27.** Let D be the set of all finite subsets of positive integers, and define $T: \mathbf{Z}^+ \to D$ by the following rule: For every integer n, $T(n) =$ the set of all of the positive divisors of n.
a. Is T one-to-one? Prove or give a counterexample.
b. Is T onto? Prove or give a counterexample.

28. Define $G: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: $G(x, y) = (2y, -x)$ for every $(x, y) \in \mathbf{R} \times \mathbf{R}$.
a. Is G one-to-one? Prove or give a counterexample.
b. Is G onto? Prove or give a counterexample.

29. Define $H: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: $H(x, y) = (x + 1, 2 - y)$ for every $(x, y) \in \mathbf{R} \times \mathbf{R}$.
a. Is H one-to-one? Prove or give a counterexample.
b. Is H onto? Prove or give a counterexample.

***H*30.** Define $J: \mathbf{Q} \times \mathbf{Q} \to \mathbf{R}$ by the rule $J(r, s) = r + \sqrt{2}s$ for each $(r, s) \in \mathbf{Q} \times \mathbf{Q}$.
a. Is J one-to-one? Prove or give a counterexample.
b. Is J onto? Prove or give a counterexample.

**** 31.** Define $F: \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ and $G: \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ as follows: For each $(n, m) \in \mathbf{Z}^+ \times \mathbf{Z}^+$,

$$F(n, m) = 3^n 5^m \quad \text{and} \quad G(n, m) = 3^n 6^m.$$

H **a.** Is F one-to-one? Prove or give a counterexample.
b. Is G one-to-one? Prove or give a counterexample.

32. a. Is $\log_8 27 = \log_2 3$? Why or why not?
b. Is $\log_{16} 9 = \log_4 3$? Why or why not?

The properties of logarithm established in 33–35 are used in Sections 11.4 and 11.5.

33. Prove that for all positive real numbers b, x, and y with $b \neq 1$,

$$\log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y.$$

34. Prove that for all positive real numbers b, x, and y with $b \neq 1$,

$$\log_b(xy) = \log_b x + \log_b y.$$

H **35.** Prove that for all real numbers a, b, and x with b and x positive and $b \neq 1$,

$$\log_b(x^a) = a \log_b x.$$

Exercises 36 and 37 use the following definition: If f: R → R and g: R → R are functions, then the function $(f+g)$: R → R is defined by the formula $(f+g)(x) = f(x) + g(x)$ for every real number x.

36. If f: $\mathbf{R} \to \mathbf{R}$ and g: $\mathbf{R} \to \mathbf{R}$ are both one-to-one, is $f+g$ also one-to-one? Justify your answer.

37. If f: $\mathbf{R} \to \mathbf{R}$ and g: $\mathbf{R} \to \mathbf{R}$ are both onto, is $f+g$ also onto? Justify your answer.

Exercises 38 and 39 use the following definition: If f: R → R is a function and c is a nonzero real number, the function $(c\cdot f)$: R → R is defined by the formula $(c\cdot f)(x) = c\cdot(f(x))$ for every real number x.

38. Let f: $\mathbf{R} \to \mathbf{R}$ be a function and c a nonzero real number. If f is one-to-one, is $c \cdot f$ also one-to-one? Justify your answer.

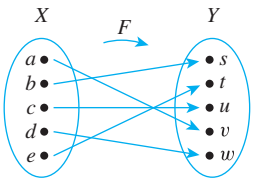
39. Let f: $\mathbf{R} \to \mathbf{R}$ be a function and c a nonzero real number. If f is onto, is $c \cdot f$ also onto? Justify your answer.

H **40.** Suppose F: $X \to Y$ is one-to-one.
a. Prove that for every subset $A \subseteq X$, $F^{-1}(F(A)) = A$.
b. Prove that for all subsets A_1 and A_2 in X, $F(A_1 \cap A_2) = F(A_1) \cap F(A_2)$.

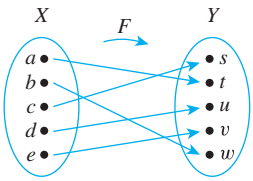
41. Suppose F: $X \to Y$ is onto. Prove that for every subset $B \subseteq Y$, $F(F^{-1}(B)) = B$.

Let $X = \{a, b, c, d, e\}$ and $Y = \{s, t, u, v, w\}$. In each of 42 and 43 a one-to-one correspondence F: $X \to Y$ is defined by an arrow diagram. In each case draw an arrow diagram for F^{-1}.

42.



43.



In 44–55 indicate which of the functions in the referenced exercise are one-to-one correspondences. For each function that is a one-to-one correspondence, find the inverse function.

44. Exercise 10a
45. Exercise 10b
46. Exercise 11a
47. Exercise 11b
48. Exercise 12a
49. Exercise 12b
50. Exercise 21
51. Exercise 22

52. Exercise 15 with the co-domain taken to be the set of all real numbers not equal to 1

53. Exercise 16 with the co-domain taken to be the set of all real numbers

54. Exercise 17 with the co-domain taken to be the set of all real numbers not equal to 3

55. Exercise 18 with the co-domain taken to be the set of all real numbers not equal to 1

56. In Example 7.2.8 a one-to-one correspondence was defined from the power set of $\{a, b\}$ to the set of all strings of 0's and 1's that have length 2. Thus the elements of these two sets can be matched up exactly, and so the two sets have the same number of elements.
a. Let $X = \{x_1, x_2, \ldots, x_n\}$ be a set with n elements. Use Example 7.2.8 as a model to

define a one-to-one correspondence from $\mathcal{P}(X)$, the set of all subsets of X, to the set of all strings of 0's and 1's that have length n.

b. In Section 9.2 we show that there are 2^n strings of 0's and 1's that have length n. What does this allow you to conclude about the number of subsets of $\mathcal{P}(X)$? (This provides an alternative proof of Theorem 6.3.1.)

***H* 57.** Write a computer algorithm to check whether a function from one finite set to another is one-to-one. Assume the existence of an independent algorithm to compute values of the function.

***H* 58.** Write a computer algorithm to check whether a function from one finite set to another is onto. Assume the existence of an independent algorithm to compute values of the function.

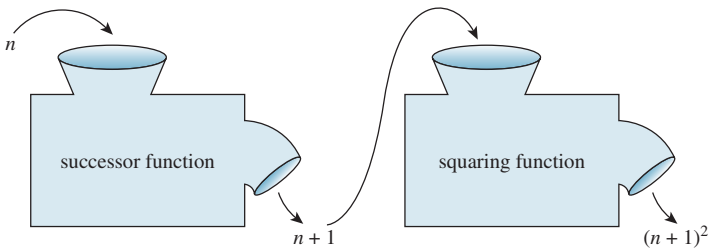
ANSWERS FOR TEST YOURSELF

1. for all x_1 and x_2 in X, if $F(x_1) = F(x_2)$ then $x_1 = x_2$ **2.** there exist elements x_1 and x_2 in X such that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$ **3.** for every element y in Y, there exists at least one element x in X such that $f(x) = y$ **4.** there exists an element y in Y such that for every element x in X, $f(x) \neq y$ **5.** logically equivalent ways of expressing what it means for a function H to be one-to-one (The second is the contrapositive of the first.) **6.** x_1 and x_2 are any *[particular but arbitrarily chosen]* elements in X with the property that $F(x_1) = F(x_2)$; $x_1 = x_2$ **7.** y is any *[particular but arbitrarily chosen]* element in Y; there exists at least one element x in X such that $F(x) = y$ **8.** show that there are concrete elements x_1 and x_2 in X with the property that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$ **9.** show that there is a concrete element y in Y with the property that $F(x) \neq y$ for any element x in X **10.** function from X to Y; both one-to-one and onto **11.** the unique element x in X such that $F(x) = y$ (in other words, $F^{-1}(y)$ is the unique preimage of y in X)

7.3 Composition of Functions

It is no paradox to say that in our most theoretical moods we may be nearest to our most practical applications. —Alfred North Whitehead

Consider two functions, the successor function and the squaring function, both defined from **Z** to **Z**, and imagine that each is represented by a machine. If the two machines are hooked up so that the output from the successor function is used as input to the squaring function, then they work together to operate as one larger machine. In this larger machine, an integer n is first increased by 1 to obtain $n + 1$; then the quantity $n + 1$ is squared to obtain $(n + 1)^2$. This is illustrated in the following drawing.



Combining functions in this way is called *composing* them; the resulting function is called the *composition* of the two functions. Note that the composition can be formed only if the output of the first function is acceptable input to the second function. That is, the range of the first function must be contained in the domain of the second function.

Definition

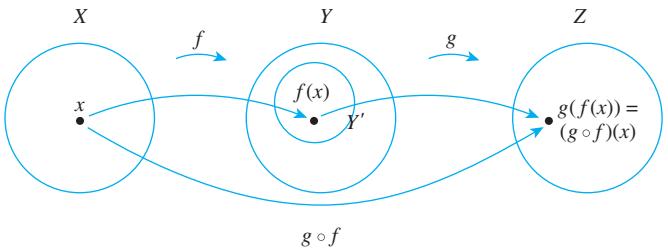
Let $f: X \to Y$ and $g: Y' \to Z$ be functions with the property that the range of f is a subset of the domain of g. Define a new function $g \circ f: X \to Z$ as follows:

$$(g \circ f)(x) = g(f(x)) \quad \text{for each } x \in X,$$

where $g \circ f$ is read "g circle f" and $g(f(x))$ is read "g of f of x." The function $g \circ f$ is called the **composition of f and g**.

Note Even though we write $g \circ f$, we put f first when we say "the composition of f and g" because an element x is acted upon first by f and then by g.

This definition is shown schematically below.



Example 7.3.1 **Composition of Functions Defined by Formulas**

Let $f: \mathbf{Z} \to \mathbf{Z}$ be the successor function and let $g: \mathbf{Z} \to \mathbf{Z}$ be the squaring function. Then $f(n) = n + 1$ for each $n \in \mathbf{Z}$ and $g(n) = n^2$ for each $n \in \mathbf{Z}$.

a. Find the compositions $g \circ f$ and $f \circ g$.

b. Is $g \circ f = f \circ g$? Explain.

Caution! Be careful not to confuse $g \circ f$ and $g(f(x))$: $g \circ f$ is the name of the function whereas $g(f(x))$ is the value of the function at x.

Solution

a. Because f sends each integer to that integer plus 1 and g sends each integer to the square of that integer, it can be helpful to think of the action of f and g as follows:

$$f(\text{any integer}) = \text{that integer} + 1 \quad \textit{[even if the integer is } g(n)\textit{]}.$$
$$g(\text{any integer}) = (\text{that integer})^2 \quad \textit{[even if the integer is } f(n)\textit{]}.$$

Thus the functions $g \circ f$ and $f \circ g$ are defined as follows:

$$(g \circ f)(n) = g(f(n)) = g(n + 1) = (n + 1)^2 \quad \text{for each } n \in \mathbf{Z},$$

and

$$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1 \quad \text{for each } n \in \mathbf{Z}.$$

b. Two functions from one set to another are equal if, and only if, they always take the same values. In this case,

$$(g \circ f)(1) = (1 + 1)^2 = 4, \text{ whereas } (f \circ g)(1) = 1^2 + 1 = 2.$$

Thus the two functions $g \circ f$ and $f \circ g$ are not equal:

$$g \circ f \neq f \circ g.$$

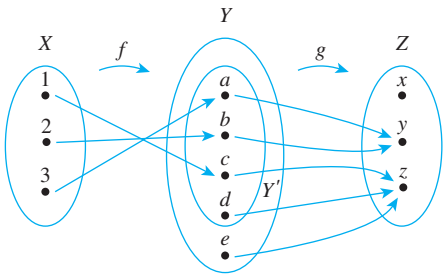
■

Note For general functions F and G, $F \circ G$ need not necessarily equal $G \circ F$ (although the two may be equal).

Example 7.3.1 illustrates the important fact that composition of functions is not a commutative operation.

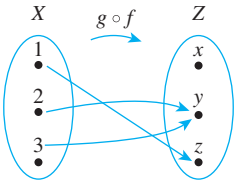
Example 7.3.2 **Composition of Functions Defined on Finite Sets**

Let $X = \{1, 2, 3\}$, $Y' = \{a, b, c, d\}$, $Y = \{a, b, c, d, e\}$, and $Z = \{x, y, z\}$. Define functions $f: X \to Y'$ and $g: Y \to Z$ by the arrow diagrams below.



Draw the arrow diagram for $g \circ f$. What is the range of $g \circ f$?

Solution To find the arrow diagram for $g \circ f$, just trace the arrows all the way across from X to Z through Y. The result is shown below.



$$(g \circ f)(1) = g(f(1)) = g(c) = z$$
$$(g \circ f)(2) = g(f(2)) = g(b) = y$$
$$(g \circ f)(3) = g(f(3)) = g(a) = y$$

The range of $g \circ f$ is $\{y, z\}$. ■

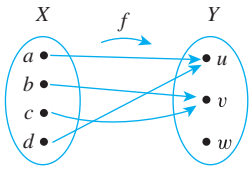
Recall that the identity function on a set X, I_X, is the function from X to X defined by the formula

$$I_X(x) = x \quad \text{for every } x \in X.$$

That is, the identity function on X sends each element of X to itself. What happens when an identity function is composed with another function?

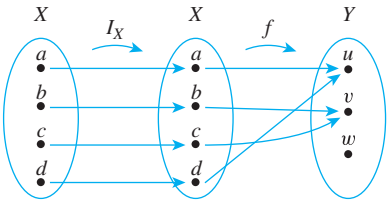
Example 7.3.3 **Composition with the Identity Function**

Let $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$, and suppose $f: X \to Y$ is given by the arrow diagram shown below.



Find $f \circ I_X$ and $I_Y \circ f$.

Solution The values of $f \circ I_X$ are obtained by tracing through the arrow diagram shown below.



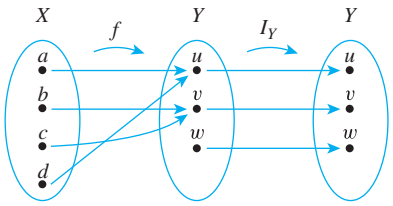
$$(f \circ I_X)(a) = f(I_X(a)) = f(a) = u$$
$$(f \circ I_X)(b) = f(I_X(b)) = f(b) = v$$
$$(f \circ I_X)(c) = f(I_X(c)) = f(c) = v$$
$$(f \circ I_X)(d) = f(I_X(d)) = f(d) = u$$

Thus, for every element x in X,

$$(f \circ I_X)(x) = f(x).$$

By definition of equality of functions, this means that $f \circ I_X = f$.

Similarly, the equality $I_Y \circ f = f$ can be verified by tracing through the arrow diagram below for each x in X and noting that in each case, $(I_Y \circ f)(x) = f(x)$.



■

More generally, the composition of any function with an identity function equals the function.

Theorem 7.3.1 Composition with an Identity Function

If f is a function from a set X to a set Y, and I_X is the identity function on X, and I_Y is the identity function on Y, then

$$\text{(a) } f \circ I_X = f \quad \text{and} \quad \text{(b) } I_Y \circ f = f.$$

Proof:

Part (a): Suppose f is a function from a set X to a set Y and I_X is the identity function on X. Then, for each x in X,

$$(f \circ I_X)(x) = f(I_X(x)) = f(x).$$

Hence, by definition of equality of functions, $f \circ I_X = f$, as was to be shown.

Part (b): This is exercise 16 at the end of this section.

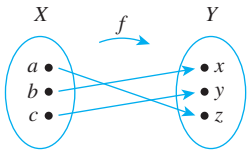
Now let f be a function from a set X to a set Y, and suppose f has an inverse function f^{-1}. Recall that f^{-1} is the function from Y to X with the property that

$$f^{-1}(y) = x \quad \Leftrightarrow \quad f(x) = y.$$

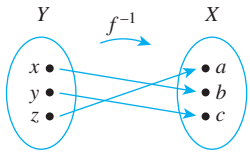
What happens when f is composed with f^{-1}? Or when f^{-1} is composed with f?

Example 7.3.4 **Composing a Function with Its Inverse**

Let $X = \{a, b, c\}$ and $Y = \{x, y, z\}$. Define $f: X \longrightarrow Y$ by the following arrow diagram.



You can see from the diagram that f is one-to-one and onto. Thus f^{-1} exists and is found by tracing the arrows backwards, as shown below.



Now $f^{-1} \circ f$ is found by following the arrows from X to Y by f and back to X by f^{-1}. If you do this, you will see that

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(z) = a$$
$$(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(x) = b$$

and

$$(f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(y) = c.$$

Thus the composition of f and f^{-1} sends each element to itself. So by definition of the identity function,

$$f^{-1} \circ f = I_X.$$

In a similar way, you can see that

$$f \circ f^{-1} = I_Y.$$ ■

More generally, the composition of any function with its inverse (if it has one) is an identity function. Intuitively, the function sends an element in its domain to an element in its co-domain and the inverse function sends it back again, so the composition of the two sends each element to itself. This reasoning is formalized in Theorem 7.3.2.

Theorem 7.3.2 Composition of a Function with Its Inverse

If $f: X \to Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \to X$, then

(a) $f^{-1} \circ f = I_X$ and (b) $f \circ f^{-1} = I_Y$.

Proof:

Part (a): Suppose $f: X \to Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \to X$. *[To show that $f^{-1} \circ f = I_X$, we must show that for each $x \in X$, $(f^{-1} \circ f)(x) = x$.]* Let x be any element in X. Then, by definition of composition of functions,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x))$$

Let

$$z = f^{-1}(f(x)).$$

By definition of inverse function,

$$f(z) = f(x),$$

(continued on page 466)

Note Recall that if b is any element of Y, then $f^{-1}(b) =$ that element a of X such that $f(a) = x$.

and, because f is one-to-one, this implies that

$$z = x.$$

Now $z = f^{-1}(f(x))$ also, and so, by substitution,

$$f^{-1}(f(x)) = x,$$

Or, equivalently,

$$(f^{-1} \circ f)(x) = x,$$

[as was to be shown].

Since x is any element of X and since $I_X(x) = x$, this proves that $f^{-1} \circ f = I_X$.

Part (b): This is exercise 17 at the end of this section.

Composition of One-to-One Functions

The composition of functions interacts in interesting ways with the properties of being one-to-one and onto. What happens, for instance, when two one-to-one functions are composed? Must their composition be one-to-one? For example, let $X = \{a, b, c\}$, $Y = \{w, x, y, z\}$, and $Z = \{1, 2, 3, 4, 5\}$, and define one-to-one functions $f: X \to Y$ and $g: Y \to Z$ as shown in the arrow diagrams of Figure 7.3.1.

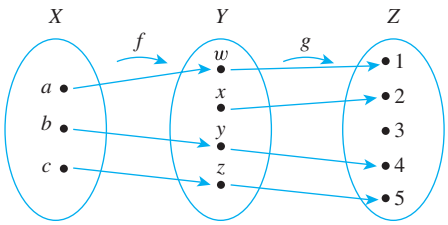


FIGURE 7.3.1

Then $g \circ f$ is the function with the arrow diagram shown in Figure 7.3.2.

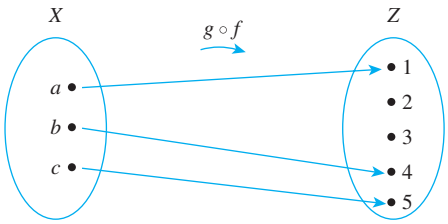


FIGURE 7.3.2

From the diagram it is clear that for these particular functions, the composition is one-to-one. This result is no accident. It turns out that the composition of two one-to-one functions is always one-to-one.

Theorem 7.3.3

If $f: X \to Y$ and $g: Y \to Z$ are both one-to-one functions, then $g \circ f$ is one-to-one.

By the method of direct proof, the proof of Theorem 7.3.3 has the following starting point and conclusion to be shown.

Starting Point: Suppose f is a one-to-one function from X to Y and g is a one-to-one function from Y to Z.

To Show: $g \circ f$ is a one-to-one function from X to Z.

The conclusion to be shown says that a certain function is one-to-one. How do you show that? The crucial step is to realize that if you substitute $g \circ f$ into the definition of one-to-one, you see that

$$g \circ f \text{ is one-to-one} \quad \Leftrightarrow \quad \forall x_1, x_2 \in X, \text{ if } (g \circ f)(x_1) = (g \circ f)(x_2) \text{ then } x_1 = x_2.$$

By the method of direct proof, then, to show $g \circ f$ is one-to-one, you

suppose x_1 and x_2 are any elements of X such that $(g \circ f)(x_1) = (g \circ f)(x_2)$,

and you

show that $x_1 = x_2$.

Now the heart of the proof begins. To show that $x_1 = x_2$, you work forward from the supposition that $(g \circ f)(x_1) = (g \circ f)(x_2)$, using the fact that f and g are both one-to-one. By definition of composition,

$$(g \circ f)(x_1) = g(f(x_1)) \quad \text{and} \quad (g \circ f)(x_2) = g(f(x_2)).$$

Since the left-hand sides of the equations are equal, so are the right-hand sides. Thus

$$g(f(x_1)) = g(f(x_2)).$$

Now just stare at the above equation for a moment. It says that

$$g(\text{something}) = g(\text{something else}).$$

Because g is a one-to-one function, any time g of one thing equals g of another thing, those two things are equal. Hence

$$f(x_1) = f(x_2).$$

But f is also a one-to-one function. Any time f of one thing equals f of another thing, those two things are equal. Therefore,

$$x_1 = x_2.$$

This is what was to be shown!

This discussion is summarized in the following formal proof.

Proof of Theorem 7.3.3:

Suppose $f: X \to Y$ and $g: Y \to Z$ are both one-to-one functions. *[We must show that $g \circ f$ is one-to-one.]* Suppose x_1 and x_2 are elements of X such that

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

[We must show that $x_1 = x_2$.] By definition of composition of functions,

$$g(f(x_1)) = g(f(x_2)).$$

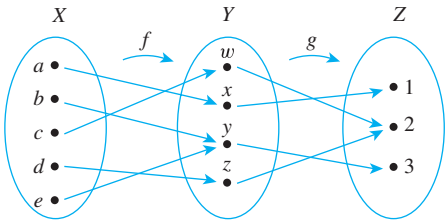
Since g is one-to-one, $f(x_1) = f(x_2)$.

And since f is one-to-one, $x_1 = x_2$

[as was to be shown]. Hence $g \circ f$ is one-to-one.

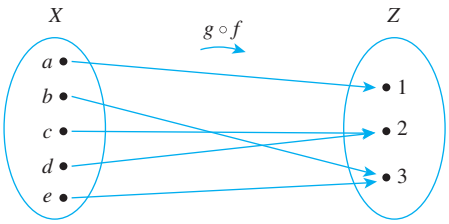
Composition of Onto Functions

Now consider what happens when two onto functions are composed. For example, let $X = \{a, b, c, d, e\}$, $Y = \{w, x, y, z\}$, and $Z = \{1, 2, 3\}$. Define onto functions f and g by the following arrow diagrams.



Then $g \circ f$ is the function with the arrow diagram shown below.

It is clear from the diagram that $g \circ f$ is onto.



It turns out that the composition of any two onto functions (that can be composed) is onto.

Theorem 7.3.4

If $f: X \to Y$ and $g: Y \to Z$ are both onto functions, then $g \circ f$ is onto.

A direct proof of Theorem 7.3.4 has the following starting point and conclusion to be shown:

Starting Point: Suppose f is an onto function from X to Y, and g is an onto function from Y to Z.

To Show: $g \circ f$ is an onto function from X to Z.

The conclusion to be shown says that a certain function is onto. How do you show that? The crucial step is to realize that if you substitute $g \circ f$ into the definition of onto, you see that

$g \circ f: X \to Z$ is onto	$\Leftrightarrow$	given any element z of Z, it is possible to find an element x of X such that $(g \circ f)(x) = z$.

Since this statement is universal, to prove it you

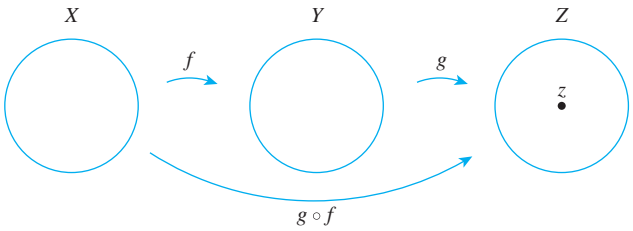
suppose z is a *[particular but arbitrarily chosen]* element of Z

and **show** that there is an element x in X such that $(g \circ f)(x) = z$.

Caution! To show that a function is onto, you *must* start with an arbitrary element of the co-domain and deduce that it is the image of some element in the domain.

Hence you must start the proof by supposing you are given a particular but arbitrarily chosen element in Z. Let us call it z. Your job is to find an element x in X such that $(g \circ f)(x) = z$.

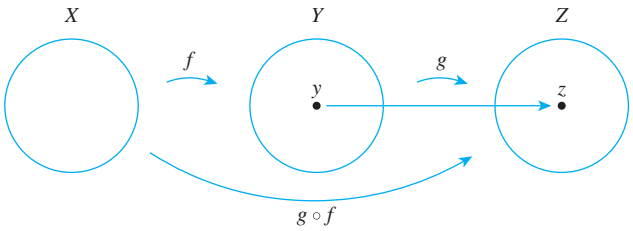
To find x, reason from the supposition that z is in Z, using the fact that both g and f are onto. Imagine arrow diagrams for the functions f and g.



You have a particular element z in Z, and you need to find an element x in X such that when x is sent over to Z by $g \circ f$, its image will be z. Now since g is onto, z is at the tip of some arrow coming from Y. That is, there is an element y in Y such that

$$g(y) = z. \tag{7.3.1}$$

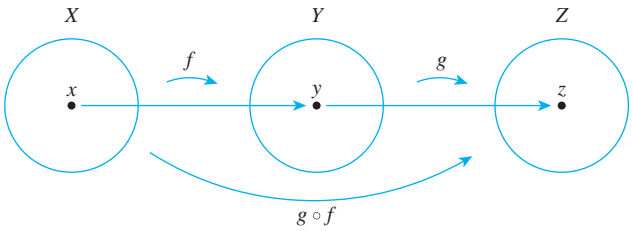
This means that the arrow diagrams can be drawn as follows:



But f also is onto, and so every element in Y is at the tip of an arrow coming from X. In particular, y is at the tip of some arrow. That is, there is an element x in X such that

$$f(x) = y. \tag{7.3.2}$$

The diagram, therefore, can be drawn as shown below.



Now just substitute equation (7.3.2) into equation (7.3.1) to obtain

$$g(f(x)) = z.$$

And by definition of $g \circ f$, this can be rewritten as

$$g(f(x)) = (g \circ f)(x).$$

Hence

$$(g \circ f)(x) = z.$$

Thus x is an element of X that is sent by $g \circ f$ to z, and so x is the element you were supposed to find.

This discussion is summarized in the following formal proof.

Proof of Theorem 7.3.4:

Suppose $f: X \to Y$ and $g: Y \to Z$ are both onto functions. *[We must show that $g \circ f$ is onto.]* Let z be any *[particular but arbitrarily chosen]* element of Z. *[We must show the existence of an element in X such that $g \circ f$ of that element equals z.]* Since g is onto, there is an element, say y, in Y such that $g(y) = z$. And since f is onto, there is an element, say x, in X such that $f(x) = y$. Hence there is an element x in X such that

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

[as was to be shown]. It follows that $g \circ f$ is onto.

Example 7.3.5 **An Incorrect "Proof" That a Function Is Onto**

To prove that a composition of onto functions is onto, a student wrote:

1. "Suppose $f: X \to Y$ and $g: Y \to Z$ are both onto. Then
2. $\quad \forall y \in Y, \exists x \in X$ such that $f(x) = y$,
3. and
4. $\quad \forall z \in Z, \exists y \in Y$ such that $f(y) = z$.
5. So
6. $\quad (g \circ f)(x) = g(f(x)) = g(y) = z$,
7. and thus $g \circ f$ is onto."

Explain the mistakes in this "proof."

Solution To show that $g \circ f$ is onto, you have to meet the following challenge: If someone gives you an element z in Z (over which you have no control), you must be able to explain how to find an element x in X such that $(g \circ f)(x) = z$. Thus a proof that $g \circ f$ is onto must start with the assumption that you have been given a particular but arbitrarily chosen element of Z. This proof does not do that.

In fact the statements in lines 2 and 4 simply restate the hypothesis that f and g are functions that are onto. The x, y, and z in these lines are local variables, with no meaning outside the quantified statements that contain them. In particular, the variable y in line 2 is unrelated to the variable y in line 4. So in line 6 it is wrong to assume that the two y's refer to the same object, which removes the justification for concluding that $g \circ f$ is onto. ■

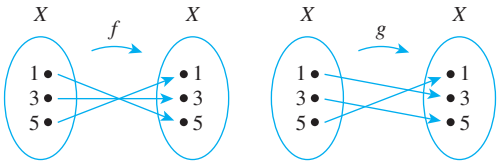
TEST YOURSELF

1. If f is a function from X to Y', g is a function from Y to Z, and $Y' \subseteq Y$, then $g \circ f$ is a function from _____ to_____, and $(g \circ f)(x) =$ _____ for every x in X.
2. If f is a function from X to Y and I_x and I_y are the identity functions from X to X and Y to Y, respectively, then $f \circ I_x =$ _____ and $I_y \circ f =$ _____.
3. If f is a one-to-one correspondence from X to Y, then $f^{-1} \circ f =$ _____ and $f \circ f^{-1} =$ _____.
4. If f is a one-to-one function from X to Y and g is a one-to-one function from Y to Z, you prove that $g \circ f$ is one-to-one by supposing that _____ and then showing that _____.
5. If f is an onto function from X to Y and g is an onto function from Y to Z, you prove that $g \circ f$ is onto by supposing that _____ and then showing that _____.

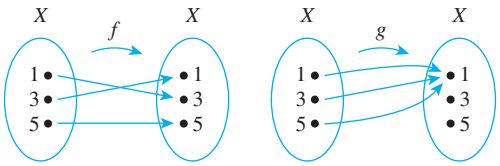
EXERCISE SET 7.3

In each of 1 and 2, functions f and g are defined by arrow diagrams. Find $g \circ f$ and $f \circ g$ and determine whether $g \circ f$ equals $f \circ g$.

1.



2.



In 3 and 4, functions F and G are defined by formulas. Find $G \circ F$ and $F \circ G$ and determine whether $G \circ F$ equals $F \circ G$.

3. $F(x) = x^3$ and $G(x) = x - 1$, for each real number x.
4. $F(x) = x^5$ and $G(x) = x^{1/5}$ for each real number x.
5. Define $f: \mathbf{R} \to \mathbf{R}$ by the rule $f(x) = -x$ for every real number x. Find $(f \circ f)(x)$.
6. Define $F: \mathbf{Z} \to \mathbf{Z}$ and $G: \mathbf{Z} \to \mathbf{Z}$ by the rules $F(a) = 7a$ and $G(a) = a \bmod 5$ for each integer a. Find $(G \circ F)(0)$, $(G \circ F)(1)$, $(G \circ F)(2)$, $(G \circ F)(3)$, and $(G \circ F)(4)$.
7. Define $L: \mathbf{Z} \to \mathbf{Z}$ and $M: \mathbf{Z} \to \mathbf{Z}$ by the rules $L(a) = a^2$ and $M(a) = a \bmod 5$ for each integer a.
   H a. Find $(L \circ M)(12)$, $(M \circ L)(12)$, $(L \circ M)(9)$, and $(M \circ L)(9)$.
   b. Is $L \circ M = M \circ L$?
8. Let S be the set of all strings in a's and b's and let $L: S \to \mathbf{Z}$ be the length function:

   For all strings $s \in S$,

   $$L(s) = \text{the number of characters in } s.$$

   Let $T: \mathbf{Z} \to \{0, 1, 2\}$ be the *mod* 3 function:

   For every integer n, $\quad T(n) = n \bmod 3$.

   a. $(T \circ L)(abaa) = ?$
   b. $(T \circ L)(baaab) = ?$
   c. $(T \circ L)(aaa) = ?$
9. Define $F: \mathbf{R} \to \mathbf{R}$ and $G: \mathbf{R} \to \mathbf{Z}$ by the following formulas: $F(x) = x^2/3$ and $G(x) = \lfloor x \rfloor$ for every $x \in \mathbf{R}$.
   a. $(G \circ F)(2) = ?$
   b. $(G \circ F)(-3) = ?$
   c. $(G \circ F)(5) = ?$
10. Define $F: \mathbf{Z} \to \mathbf{Z}$ and $G: \mathbf{Z} \to \mathbf{Z}$ by the rules $F(n) = 2n$ and $G(n) = \lfloor n/2 \rfloor$ for every integer n.
    a. Find $(G \circ F)(8)$, $(F \circ G)(8)$, $(G \circ F)(3)$, and $(F \circ G)(3)$.
    b. Is $G \circ F = F \circ G$? Explain.
11. Define $F: \mathbf{R} \to \mathbf{R}$ and $G: \mathbf{R} \to \mathbf{R}$ by the rules $F(n) = 3x$ and $G(n) = \lceil x/3 \rceil$ for every real number x.
    a. Find $(G \circ F)(6)$, $(F \circ G)(6)$, $(G \circ F)(1)$, and $(F \circ G)(1)$.
    b. Is $G \circ F = F \circ G$? Explain.

The functions of each pair in 12–14 are inverse to each other. For each pair, check that both compositions give the identity function.

12. $F: \mathbf{R} \to \mathbf{R}$ and $F^{-1}\ \mathbf{R} \to \mathbf{R}$ are defined by

$$F(x) = 3x + 2 \quad \text{and} \quad F^{-1}(y) = \frac{y - 2}{3},$$

for every $y \in \mathbf{R}$.

13. $G: \mathbf{R}^+ \to \mathbf{R}^+$ and $G^{-1}: \mathbf{R}^+ \to \mathbf{R}^+$ are defined by

$$G(x) = x^2 \quad \text{and} \quad G^{-1}(x) = \sqrt{x}$$

for every $x \in \mathbf{R}^+$.

14. H and H^{-1} are both defined from $\mathbf{R} - \{1\}$ to $\mathbf{R} - \{1\}$ by the formula

$$H(x) = H^{-1}(x) = \frac{x+1}{x-1}, \quad \text{for each } x \in \mathbf{R} - \{1\}.$$

15. Explain how it follows from the definition of logarithm that

a. $\log_b(b^x) = x$, for every real number x.

b. $b^{\log_b x} = x$, for every positive real number x.

H 16. Prove Theorem 7.3.1(b): If f is any function from a set X to a set Y, then $I_Y \circ f = f$, where I_Y is the identity function on Y.

17. Prove Theorem 7.3.2(b): If $f: X \to Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \to X$, then $f \circ f^{-1} = I_Y$, where I_Y is the identity function on Y.

18. Suppose Y and Z are sets and $g: Y \to Z$ is a one-to-one function. This means that if g takes the same value on any two elements of Y, then those elements are equal. Thus, for example, if a and b are elements of Y and $g(a) = g(b)$, then it can be inferred that $a = b$. What can be inferred in the following situations?

a. s_k and s_m are elements of Y and $g(s_k) = g(s_m)$.

b. $z/2$ and $t/2$ are elements of Y and $g(z/2) = g(t/2)$.

c. $f(x_1)$ and $f(x_2)$ are elements of Y and $g(f(x_1)) = g(f(x_2))$.

19. If $f: X \to Y$ and $g: Y \to Z$ are functions and $g \circ f$ is one-to-one, must g be one-to-one? Prove or give a counterexample.

20. If $f: X \to Y$ and $g: Y \to Z$ are functions and $g \circ f$ is onto, must f be onto? Prove or give a counterexample.

H 21. If $f: X \to Y$ and $g: Y \to Z$ are functions and $g \circ f$ is one-to-one, must f be one-to-one? Prove or give a counterexample.

H 22. If $f: X \to Y$ and $g: Y \to Z$ are functions and $g \circ f$ is onto, must g be onto? Prove or give a counterexample.

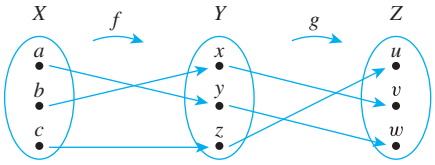
23. Let $f: W \to X$, $g: X \to Y$, and $h: Y \to Z$ be functions. Must $h \circ (g \circ f) = (h \circ g) \circ f$? Prove or give a counterexample.

24. True or False? Given any set X and given any functions $f: X \to X$, $g: X \to X$, and $h: X \to X$, if h is one-to-one and $h \circ f = h \circ g$, then $f = g$. Justify your answer.

25. True or False? Given any set X and given any functions $f: X \to X$, $g: X \to X$, and $h: X \to X$, if h is one-to-one and $f \circ h = g \circ h$, then $f = g$. Justify your answer.

In 26 and 27 find $(g \circ f)^{-1}$, g^{-1}, f^{-1}, and $f^{-1} \circ g^{-1}$, and state how $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ are related.

26. Let $X = \{a, b, c\}$, $Y = \{x, y, z\}$, and $Z = \{u, v, w\}$. Define $f: X \to Y$ and $g: Y \to Z$ by the arrow diagrams below.



27. Define $f: \mathbf{R} \to \mathbf{R}$ and $g: \mathbf{R} \to \mathbf{R}$ by the formulas

$$f(x) = x + 3 \quad \text{and} \quad g(x) = -x \quad \text{for each } x \in \mathbf{R}.$$

28. Prove or give a counterexample: If $f: X \to Y$ and $g: Y \to X$ are functions such that $g \circ f = I_X$ and $f \circ g = I_Y$, then f and g are both one-to-one and onto and $g = f^{-1}$.

H 29. Suppose $f: X \to Y$ and $g: Y \to Z$ are both one-to-one and onto. Prove that $(g \circ f)^{-1}$ exists and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

30. Let $f: X \to Y$ and $g: Y \to Z$. Is the following property true or false? For every subset C in Z, $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$. Justify your answer.

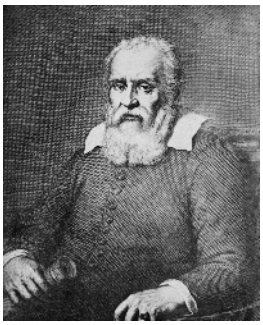
ANSWERS FOR TEST YOURSELF

1. X; Z; $g(f(x))$ **2.** f; f **3.** I_X; I_Y **4.** x_1 and x_2 are any *[particular but arbitrarily chosen]* elements in X with the property that $(g \circ f)(x_1) = (g \circ f)(x_2)$; $x_1 = x_2$

5. z is any *[particular but arbitrarily chosen]* element in Z; there exists at least one element x in X such that $(g \circ f)(x) = z$

7.4 Cardinality with Applications to Computability

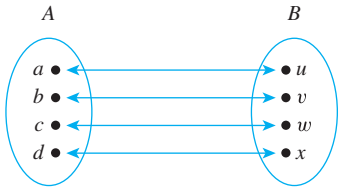
There are as many squares as there are numbers because they are just as numerous as their roots. —Galileo Galilei, 1632



wynnter/Getty Images

Galileo Galilei (1564–1642)

The term *cardinal number* refers to the size of a set ("This set has *eight* elements"), whereas the term *ordinal number* refers to the order of an element in a sequence ("This is the *eighth* element in the row"). The mathematical definition of cardinal number is based on the use of fingers or tally marks to represent numbers. For instance, small children often indicate their age by holding up the same number of fingers as the years of their life, and adults frequently use one tally mark to correspond to each vote received by a candidate in an election. As was discussed in Section 7.2, a pairing of the elements of two sets is called a one-to-one correspondence. We say that two finite sets whose elements can be paired by a one-to-one correspondence have the *same size*. This is illustrated by the following diagram.



The elements of set A can be put into one-to-one correspondence with the elements of B.

Now a *finite set* is one that has no elements at all or that can be put into one-to-one correspondence with a set of the form $\{1, 2, \ldots, n\}$ for some positive integer n. By contrast, an *infinite set* is a nonempty set that cannot be put into one-to-one correspondence with $\{1, 2, \ldots, n\}$ for any positive integer n. Suppose that, as suggested by the quote from Galileo at the beginning of this section, we extend the concept of size to infinite sets by saying that one infinite set has the same size as another if, and only if, the first set can be put into one-to-one correspondence with the second. What consequences follow from such a definition? Do all infinite sets have the same size, or are some infinite sets larger than others? These are the questions we address in this section. The answers are sometimes surprising and have the interesting consequence that there are functions defined on the set of integers whose values cannot be computed on a computer.

Definition

Let A and B be any sets. ***A* has the same cardinality as *B*** if, and only if, there is a one-to-one correspondence from A to B. In other words, A has the same cardinality as B if, and only if, there is a function f from A to B that is one-to-one and onto.

The following theorem gives some basic properties of cardinality, most of which follow from statements proved earlier about one-to-one and onto functions.

Theorem 7.4.1 Properties of Cardinality

For all sets A, B, and C:

a. **Reflexive property of cardinality:** A has the same cardinality as A.

b. **Symmetric property of cardinality:** If A has the same cardinality as B, then B has the same cardinality as A.

(continued on page 474)

c. **Transitive property of cardinality:** If A has the same cardinality as B and B has the same cardinality as C, then A has the same cardinality as C.

Proof:

Part (a), Reflexivity: Suppose A is any set. *[To show that A has the same cardinality as A, we must show there is a one-to-one correspondence from A to A.]* Consider the identity function I_A from A to A. This function is one-to-one because if x_1 and x_2 are any elements in A with $I_A(x_1) = I_A(x_2)$, then, by definition of I_A, $x_1 = x_2$. The identity function is also onto because if y is any element of A, then $y = I_A(y)$ by definition of I_A. Hence I_A is a one-to-one correspondence from A to A. *[So there exists a one-to-one correspondence from A to A, as was to be shown.]*

Part (b), Symmetry: Suppose A and B are any sets and A has the same cardinality as B. *[We must show that B has the same cardinality as A.]* Since A has the same cardinality as B, there is a function f from A to B that is one-to-one and onto. But then, by Theorems 7.2.2 and 7.2.3, there is a function f^{-1} from B to A that is also one-to-one and onto. Hence B has the same cardinality as A *[as was to be shown].*

Part (c), Transitivity: Suppose A, B, and C are any sets and A has the same cardinality as B and B has the same cardinality as C. *[We must show that A has the same cardinality as C.]* Since A has the same cardinality as B, there is a function f from A to B that is one-to-one and onto, and since B has the same cardinality as C, there is a function g from B to C that is one-to-one and onto. But then, by Theorems 7.3.3 and 7.3.4, $g \circ f$ is a function from A to C that is one-to-one and onto. Hence A has the same cardinality as C *[as was to be shown].*

Note that Theorem 7.4.1(b) makes it possible to say simply that two sets have the same cardinality instead of always having to say that one set has the same cardinality as another. That is, the following definition can be made.

Definition

A and B **have the same cardinality** if, and only if, A has the same cardinality as B or B has the same cardinality as A.

The following example illustrates a very important property of infinite sets—namely, that an infinite set can have the same cardinality as a proper subset of itself. This property is sometimes taken as the definition of infinite set. The example shows that even though it may seem reasonable to say that there are twice as many integers as there are even integers, the elements of the two sets can be matched up exactly, and so, according to the definition, the two sets have the same cardinality.

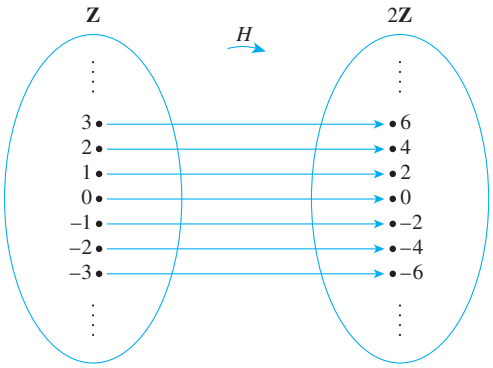
Example 7.4.1 **An Infinite Set and a Proper Subset Can Have the Same Cardinality**

Let $2\mathbf{Z}$ be the set of all even integers. Prove that $2\mathbf{Z}$ and $\mathbf{Z}$ have the same cardinality.

Solution Consider the function H from $\mathbf{Z}$ to $2\mathbf{Z}$ defined as follows:

$$H(n) = 2n \quad \text{for each } n \in \mathbf{Z}.$$

A (partial) arrow diagram for H is shown below.



To show that H is one-to-one, suppose $H(n_1) = H(n_2)$ for some integers n_1 and n_2. Then $2n_1 = 2n_2$ by definition of H, and dividing both sides by 2 gives $n_1 = n_2$. Hence h is one-to-one.

To show that H is onto, suppose m is any element of $2\mathbf{Z}$. Then m is an even integer, and so $m = 2k$ for some integer k. It follows that $H(k) = 2k = m$. Thus there exists k in $\mathbf{Z}$ with $H(k) = m$, and hence H is onto.

Note So there are "as many" even integers as there are integers!

Therefore, by definition of cardinality, $\mathbf{Z}$ and $2\mathbf{Z}$ have the same cardinality. ■

In Section 9.4 we will show that a function from one finite set to another set of the same size is one-to-one if, and only if, it is onto. This result does not hold for infinite sets. Although it is true that for two infinite sets to have the same cardinality there must exist a function from one to the other that is both one-to-one and onto, it is also always the case that:

> If A and B are infinite sets with the same cardinality, then there exist functions from A to B that are one-to-one but not onto and functions from A to B that are onto but not one-to-one.

For instance, since the function H in Example 7.4.1 is one-to-one and onto, $\mathbf{Z}$ and $2\mathbf{Z}$ have the same cardinality. But the "inclusion function" I from $2\mathbf{Z}$ to $\mathbf{Z}$, given by $I(n) = n$ for all even integers n, is one-to-one but not onto. And the function J from $\mathbf{Z}$ to $2\mathbf{Z}$ defined by $J(n) = 2\lfloor n/2 \rfloor$, for each integer n, is onto but not one-to-one. (See exercise 6 at the end of this section.)

Countable Sets

The most basic of all infinite sets is $\mathbf{Z}^+$ the set of counting numbers $\{1, 2, 3, 4, \ldots\}$. A set A having the same cardinality as this set is called *countably infinite*. The reason is that the one-to-one correspondence between the two sets can be used to "count" the elements of A: If F is a one-to-one and onto function from $\mathbf{Z}^+$ to A, then $F(1)$ can be designated as the first element of A, $F(2)$ as the second element of A, $F(3)$ as the third element of A, and so forth. This is illustrated graphically in Figure 7.4.1 on the next page. Because F is one-to-one, no element is ever counted twice, and because it is onto, every element of A is counted eventually.

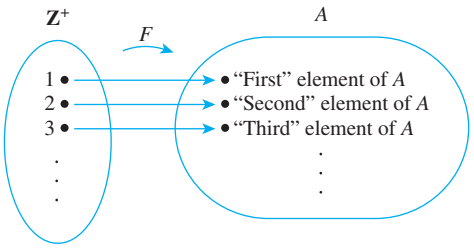


FIGURE 7.4.1 "Counting" a Countably Infinite Set

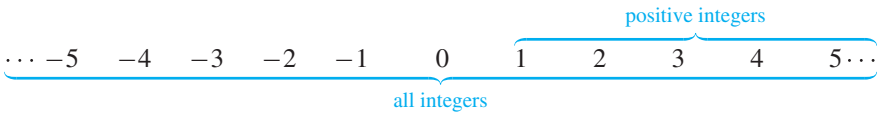
Definition

A set is **finite** if, and only if, it is the empty set or can be put into one-to-one correspondence with a set of the form $\{1, 2, \ldots, n\}$ for some positive integer n. A set is **countably infinite** if, and only if, it has the same cardinality as the set of positive integers $\mathbf{Z}^+$. A set is **countable** if, and only if, it is finite or countably infinite. A set that is not countable is called **uncountable**.

Example 7.4.2 **Countability of Z, the Set of All Integers**

Show that $\mathbf{Z}$, the set of all integers, is countable.

Solution The set $\mathbf{Z}$ is certainly not finite, so if it is countable, it must be because it is countably infinite. To show that $\mathbf{Z}$ is countably infinite, find a function from the positive integers $\mathbf{Z}^+$ to $\mathbf{Z}$ that is one-to-one and onto. This seems to contradict common sense because judging from the diagram below, there appear to be more than twice as many integers than there are positive integers.



But you were alerted that results in this section might be surprising. Try to think how you might "count" the set of all integers.

One way is to start in the middle and work outward systematically. Let the first integer be 0, the second 1, the third −1, the fourth 2, the fifth −2, and so forth, as shown in Figure 7.4.2, starting at 0 and swinging outward in back-and-forth arcs from positive to negative integers and back again, picking up one additional integer at each swing.

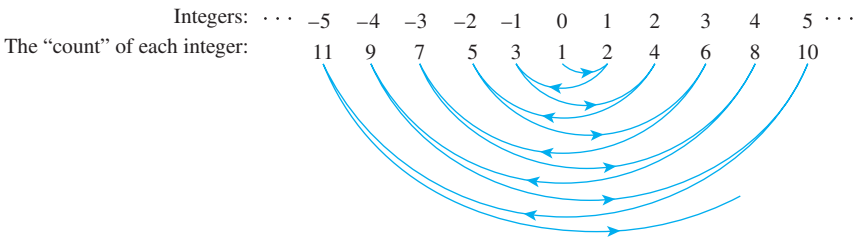


FIGURE 7.4.2 "Counting" the Set of All Integers

It is clear from the diagram that no integer is counted twice (so the function is one-to-one) and every integer is counted eventually (so the function is onto). Consequently, this diagram defines a function from $\mathbf{Z}^+$ to $\mathbf{Z}$ that is one-to-one and onto. Even though in one

sense there seem to be more integers than positive integers, the elements of the two sets can be paired up one for one. It follows by definition of cardinality that $\mathbf{Z}^+$ has the same cardinality as $\mathbf{Z}$. Thus $\mathbf{Z}$ is countably infinite and hence countable.

The diagrammatic description of the previous function is acceptable as given. You can check, however, that the function can also be described by the explicit formula

$$F(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is an even positive integer} \\ -\dfrac{n-1}{2} & \text{if } n \text{ is an odd positive integer.} \end{cases}$$

■

Example 7.4.3 **Countability of 2Z, the Set of All Even Integers**

Show that $2\mathbf{Z}$, the set of all even integers, is countable.

Solution Example 7.4.2 showed that $\mathbf{Z}^+$ has the same cardinality as $\mathbf{Z}$, and Example 7.4.1 showed that $\mathbf{Z}$ has the same cardinality as $2\mathbf{Z}$. Thus, by the transitive property of cardinality, $\mathbf{Z}^+$ has the same cardinality as $2\mathbf{Z}$. It follows by definition of countably infinite that $2\mathbf{Z}$ is countably infinite and hence countable. ■

The Search for Larger Infinities: The Cantor Diagonalization Process

Every infinite set we have discussed so far has been countably infinite. Do any larger infinities exist? Are there uncountable sets? Here is one candidate.

Imagine the number line as shown below.

As noted in Section 1.2, the integers are spread along the number line at discrete intervals. On the other hand, the rational numbers are dense along the number line. Between any two distinct rational numbers is another rational number, which implies that there are infinitely many rational numbers between any two distinct rational numbers no matter how close they are to each other. (See exercise 17 at the end of this section or exercise 20 in Section 4.3.) So, because there seem to be vastly more rational numbers than integers, it would be natural to conjecture that the infinity of the set of rational numbers is larger than the infinity of the set of integers.

Amazingly, this conjecture is false. Despite the fact that the rational numbers are crowded onto the number line whereas the integers are quite separated, the set of all rational numbers can be put into one-to-one correspondence with the set of integers. The next example gives part of a proof of this fact. It shows that the set of all positive rational numbers can be put into one-to-one correspondence with the set of all positive integers. In exercise 16 at the end of this section you are asked to use this result, together with a technique similar to that of Example 7.4.2, to show that the set of *all* rational numbers is countable.

Example 7.4.4 **The Set of All Positive Rational Numbers Is Countable**

Show that $\mathbf{Q}^+$, the set of all positive rational numbers, is countable.

Solution Display the elements of the set $\mathbf{Q}^+$ in a grid as shown in Figure 7.4.3 on the next page.

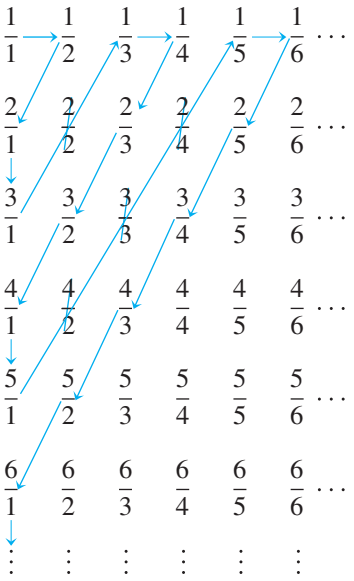


FIGURE 7.4.3

Define a function F from $\mathbf{Z}^+$ to $\mathbf{Q}^+$ by starting to count at $\frac{1}{1}$ and following the arrows as indicated, skipping over any number that has already been counted.

To be specific: Set $F(1) = 1$, $F(2) = \frac{1}{2}$, $F(3) = \frac{2}{1}$, and $F(4) = \frac{3}{1}$. Then skip $\frac{2}{2}$ since $\frac{2}{2} = \frac{1}{1}$, which was counted already. After that, set $F(5) = \frac{1}{3}$, $F(6) = \frac{1}{4}$, $F(7) = \frac{2}{3}$, $F(8) = \frac{3}{2}$, $F(9) = \frac{4}{1}$, and $F(10) = \frac{5}{1}$. Then skip $\frac{4}{2}$, $\frac{3}{3}$, and $\frac{2}{4}$ (since $\frac{4}{2} = \frac{2}{1}$, $\frac{3}{3} = \frac{1}{1}$, and $\frac{2}{4} = \frac{1}{2}$), and set $F(11) = \frac{1}{5}$. Continue in this way, defining $F(n)$ for each positive integer n.

Note that every positive rational number appears somewhere in the grid, and the counting procedure is set up so that every point in the grid is reached eventually. Thus the function F is onto. Also, skipping numbers that have already been counted ensures that no number is counted twice. Thus F is one-to-one. Consequently, F is a function from $\mathbf{Z}^+$ to $\mathbf{Q}^+$ that is one-to-one and onto, and so $\mathbf{Q}^+$ is countably infinite and hence countable. ■

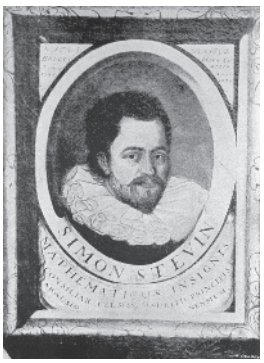
al-Kashi
(1380–1429)

In 1874 the German mathematician Georg Cantor achieved success in the search for a larger infinity by showing that the set of all real numbers is uncountable. His method of proof was somewhat complicated, however. We give a proof of the uncountability of the set of all real numbers between 0 and 1 using a simpler technique introduced by Cantor in 1891 and now called the **Cantor diagonalization process**. Over the intervening years, this technique and variations on it have been used to establish a number of important results in logic and the theory of computation.

Before stating and proving Cantor's theorem, we note that every real number is a measure of location on a number line. Each can be represented by a decimal expansion of the form

$$a_0.a_1a_2a_3\ldots,$$

where a_0 is an integer (positive, negative, or zero) and for each $i \geq 1$, a_i is an integer from 0 through 9. This way of thinking about numbers was developed over several centuries by mathematicians in the Chinese, Hindu, and Islamic worlds, culminating in the work of Ghiyāth al-Dīn Jamshīd al-Kashi in 1427. In Europe it was first clearly formulated and successfully promoted by the Flemish mathematician Simon Stevin in 1585. We illustrate the concept with an example.



Bettmann/Getty Images

Simon Stevin
(1548–1620)

Consider the point P in Figure 7.4.4. Figure 7.4.4(a) shows P located between 1 and 2. When the interval from 1 to 2 is divided into ten equal subintervals (see Figure 7.4.4(b)), P is seen to lie between 1.6 and 1.7. If the interval from 1.6 to 1.7 is itself divided into ten equal subintervals (see Figure 7.4.4(c)), the P is seen to lie between 1.62 and 1.63 but closer to 1.62 than to 1.63. So the first three digits of the decimal expansion for P are 1.62.

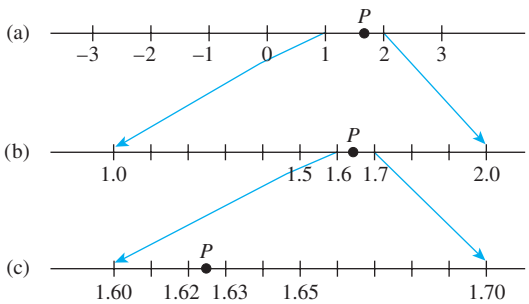


FIGURE 7.4.4

Assuming that any interval of real numbers, no matter how small, can be divided into ten equal subintervals, the process of obtaining additional digits in the decimal expansion for P can, in theory, be repeated indefinitely. At any stage if P is seen to be a subdivision point, then all further digits in the expansion may be taken to be 0. If not, then the process gives an expansion with an infinite number of digits.

The resulting decimal representation for P is unique except for numbers that end in infinitely repeating 9's or infinitely repeating 0's. For example (see exercise 25 at the end of this section), it can be proved that

$$0.199999\ldots = 0.200000\ldots$$

Let us agree to express any such decimal in the form that ends in all 0's so that we will have a unique representation for every real number.

Theorem 7.4.2 (Cantor)

The set of all real numbers between 0 and 1 is uncountable.

Proof (by contradiction): Suppose the set of all real numbers between 0 and 1 is countable. Then the decimal representations of these numbers can be written in a list as follows:

$$\begin{gathered}
0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots \\
0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots \\
0.a_{31}a_{32}a_{33}\cdots a_{3n}\cdots \\
\vdots \\
0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots \\
\vdots
\end{gathered}$$

[We will derive a contradiction by showing that there is a number between 0 and 1 that does not appear on this list.]

(continued on page 480)

For each pair of positive integers i and j, the jth decimal digit of the ith number on the list is a_{ij}. In particular, the first decimal digit of the first number on the list is a_{11}, the second decimal digit of the second number on the list is a_{22}, and so forth. As an example, suppose the list of real numbers between 0 and 1 starts out as follows:

$$\begin{array}{llllllllll}
0. & \textcircled{2} & 0 & 1 & 4 & 8 & 8 & 0 & 2 \ldots \\
0. & 1 & \textcircled{1} & 6 & 6 & 6 & 0 & 2 & 1 \ldots \\
0. & 0 & 3 & \textcircled{3} & 5 & 3 & 3 & 2 & 0 \ldots \\
0. & 9 & 6 & 7 & \textcircled{7} & 6 & 8 & 0 & 9 \ldots \\
0. & 0 & 0 & 0 & 3 & \textcircled{1} & 0 & 0 & 2 \ldots \\
 & & & & \vdots & & & &
\end{array}$$

The diagonal elements are circled: a_{11} is 2, a_{22} is 1, a_{33} is 3, a_{44} is 7, a_{55} is 1, and so forth.

Construct a new decimal number $d = 0.d_1d_2d_3 \cdots d_n \cdots$ as follows:

$$d_n = \begin{cases} 1 & \text{if } a_{nn} \neq 1 \\ 2 & \text{if } a_{nn} = 1. \end{cases}$$

In the previous example,

$$\begin{aligned}
&d_1 \text{ is 1 because } a_{11} = 2 \neq 1, \\
&d_2 \text{ is 2 because } a_{22} = 1, \\
&d_3 \text{ is 1 because } a_{33} = 3 \neq 1, \\
&d_4 \text{ is 1 because } a_{44} = 7 \neq 1, \\
&d_5 \text{ is 2 because } a_{55} = 1,
\end{aligned}$$

and so forth. Hence d would equal 0.12112….

The crucial observation is that for *each integer n*, *d differs in the nth decimal position from the nth number on the list*. But this implies that d is not on the list! In other words, d is a real number between 0 and 1 that is not on the list of *all* real numbers between 0 and 1. This contradiction shows the falseness of the supposition that the set of all numbers between 0 and 1 is countable. Hence the set of all real numbers between 0 and 1 is uncountable *[as was to be shown]*.

Along with demonstrating the existence of an uncountable set, Cantor developed a whole arithmetic theory of infinite sets of various sizes. One of the most basic theorems of the theory states that any subset of a countable set is countable.

Theorem 7.4.3

Any subset of any countable set is countable.

Proof: Let A be a particular but arbitrarily chosen countable set and let B be any subset of A. *[We must show that B is countable.]* Either B is finite or it is infinite. If B is finite, then B is countable by definition of countable, and we are done. So suppose B is infinite. Since A is countable, the distinct elements of A can be represented as a sequence

$$a_1, a_2, a_3, \ldots.$$

Define a function $g: \mathbf{Z}^+ \to B$ inductively as follows:

1. Search sequentially through elements of $a_1, a_2, a_3, \ldots$ until an element of B is found. *[This must happen eventually since $B \subseteq A$ and $B \neq \emptyset$.]* Call that element $g(1)$.
2. For each integer $k \geq 2$, suppose $g(k-1)$ has been defined. Then $g(k-1) = a_i$ for some a_i in $\{a_1, a_2, a_3, \ldots\}$. Starting with $a_i + 1$, search sequentially through $a_i + 1, a_i + 2, a_i + 3, \ldots$ trying to find an element of B. One must be found eventually because B is infinite, and $\{g(1), g(2), \ldots, g(k-1)\}$ is a finite set. When an element of B is found, define it to be $g(k)$.

By (1) and (2) above, the function g is defined for each positive integer.

Since the elements of $a_1, a_2, a_3, \ldots$ are all distinct, g is one-to-one. Furthermore, the searches for elements of B are sequential: Each picks up where the previous one left off. Thus every element of A is reached during some search. Moreover, all the elements of B are located somewhere in the sequence $a_1, a_2, a_3, \ldots$, and so every element of B is eventually found and made the image of some integer. Hence g is onto. These remarks show that g is a one-to-one correspondence from $\mathbf{Z}^+$ to B. So B is countably infinite and thus countable *[as was to be shown]*.

Note If $g(k-1) = a_i$, then $g(k)$ could also be defined by applying the well-ordering principle for the integers to the set $\{n \in \mathbf{Z} | n > i \text{ and } a_i \in B\}$.

An immediate consequence of Theorem 7.4.3 is the following corollary.

Corollary 7.4.4

Any set with an uncountable subset is uncountable.

Proof: Consider the following equivalent phrasing of Theorem 7.4.3: For every set S and for every subset A of S, if S is countable, then A is countable. The contrapositive of this statement is logically equivalent to it and states: For every set S and for every subset A of S, if A is uncountable then S is uncountable. Since this is an equivalent phrasing for the corollary, the corollary is proved.

Corollary 7.4.4 implies that the set of all real numbers is uncountable because the subset of numbers between 0 and 1 is uncountable. In fact, as Example 7.4.5 shows, the set of all real numbers has the same cardinality as the set of all real numbers between 0 and 1! This fact is further explored in exercises 13 and 14 at the end of this section.

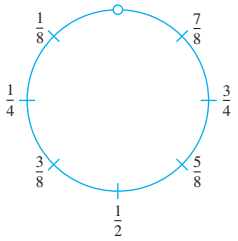
Example 7.4.5 **The Cardinality of the Set of All Real Numbers**

Show that the set of all real numbers has the same cardinality as the set of real numbers between 0 and 1.

Solution Let S be the open interval of real numbers between 0 and 1:

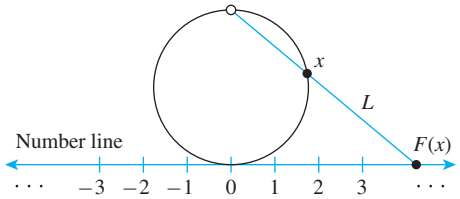
$$S = \{x \in \mathbf{R} | 0 < x < 1\}.$$

Imagine picking up S and bending it into a circle as shown below. Since S does not include either endpoint 0 or 1, the top-most point of the circle is omitted from the drawing.



Define a function $F: S \to \mathbf{R}$ as follows:

Draw a number line and place the interval, S, somewhat enlarged and bent into a circle, tangent to the number line at the point 0. This is shown below.



For each point x on the circle representing S, draw a straight line L through the top-most point of the circle and x, and let $F(x)$ be the point of intersection of L and the number line. ($F(x)$ is called the *projection* of x onto the number line.)

It is clear from the geometry of the situation that distinct points on the circle go to distinct points on the number line, so F is one-to-one. In addition, given any point y on the number line, a line can be drawn through y and the top-most point of the circle. This line must intersect the circle at some point x, and, by definition, $y = F(x)$. Thus F is onto. Hence F is a one-to-one correspondence from S to $\mathbf{R}$, and so S and $\mathbf{R}$ have the same cardinality. ■

The combination of Example 7.4.5 and Theorem 7.4.2 shows that the set of all real numbers is uncountable, which implies that there is an infinite set whose cardinality is "greater" than the infinity of the set of positive integers. In exercise 35, you are asked to prove that any set and its power set have different cardinalities. And because there is a one-to-one function from any set to its power set (the function that takes each element a to the singleton set $\{a\}$), this implies that the cardinality of any set is "less than" the cardinality of its power set. As a result, you can create an infinite sequence of larger and larger infinities! For example, you could begin with $\mathbf{Z}$, the set of all integers, and take $\mathbf{Z}$, $\mathcal{P}(\mathbf{Z})$, $\mathcal{P}(\mathcal{P}(\mathbf{Z}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbf{Z})))$, and so forth.

Application: Cardinality and Computability

Knowledge of the countability and uncountability of certain sets can be used to answer a question of computability. We begin by showing that a certain set is countable.

Example 7.4.6 **Countability of the Set of Computer Programs in a Computer Language**

Show that the set of all computer programs in a given computer language is countable.

Solution This result is a consequence of the fact that any computer program in any language can be regarded as a finite string of symbols in the (finite) alphabet of the language.

Given any computer language, let P be the set of all computer programs in the language. Either P is finite or P is infinite. If P is finite, then P is countable and we are done. If P is infinite, set up a binary code to translate the symbols of the alphabet of the language into strings of 0's and 1's. (For instance, either the seven-bit American Standard Code for Information Interchange, known as ASCII, or the eight-bit Extended Binary-Coded Decimal Interchange Code, known as EBCDIC, might be used.)

For each program in P, use the code to translate all the symbols in the program into 0's and 1's. Order these strings by length, putting shorter before longer, and order all strings of a given length by regarding each string as a binary number and writing the numbers in ascending order.

Define a function $F: \mathbf{Z}^+ \to P$ by specifying that

$$F(n) = \text{the } n\text{th program in the list} \quad \text{for each } n \in \mathbf{Z}^+.$$

By construction, F is one-to-one and onto, and so P is countably infinite and hence countable.

As a simple example, suppose the following are all the programs in P that translate into bit strings of length less than or equal to 5:

$$10111,\ 11,\ 0010,\ 1011,\ 01,\ 00100,\ 1010,\ 00010.$$

Ordering these by length gives

$$\begin{aligned} &\textit{length 2:}\ 11, 01\\ &\textit{length 4:}\ 0010, 1011, 1010\\ &\textit{length 5:}\ 10111, 00100, 00010 \end{aligned}$$

And ordering those of each given length by the size of the binary number they represent gives

$$\begin{aligned} 01 &= F(1)\\ 11 &= F(2)\\ 0010 &= F(3)\\ 1010 &= F(4)\\ 1011 &= F(5)\\ 00010 &= F(6)\\ 00100 &= F(7)\\ 10111 &= F(8) \end{aligned}$$

Note that when viewed purely as numbers and ignoring leading zeros, $0010 = 00010$. This illustrates why it is important to order the strings by length before arranging them in ascending numeric order because otherwise the values of F would not be uniquely determined. ■

The final example of this section shows that a certain set is uncountable and hence that there must exist a noncomputable function.

Example 7.4.7 **The Cardinality of a Set of Functions and Computability**

a. Let T be the set of all functions from the positive integers to the set {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. Show that T is uncountable.

b. Derive the consequence that there are noncomputable functions. Specifically, show that for any computer language there must be a function F from $\mathbf{Z}^+$ to {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} with the property that no computer program can be written in the language to take arbitrary values as input and output the corresponding function values.

Solution

a. Let S be the set of all real numbers between 0 and 1. As noted before, any number in S can be represented in the form

$$0.a_1a_2a_3 \ldots a_n \ldots,$$

where each a_i is an integer from 0 to 9. This representation is unique if decimals that end in all 9's are omitted.

Define a function F from S to a subset of T as follows:

$$F(0.a_1a_2a_3 \ldots a_n \ldots) = \text{the function that sends each positive integer } n \text{ to } a_n.$$

Note As an example, let $G = F(0.2901\ldots)$. Then $G(1) = 2$, $G(2) = 9$, $G(3) = 0$, $G(4) = 1$, and so forth.

Choose the co-domain of F to be exactly that subset of T that makes F onto, recalling that T is the set of all functions from $\mathbf{Z}^+$ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. In other words, define the co-domain of F to equal the image of F. Now F is one-to-one because in order for the functions $F(x_1)$ and $F(x_2)$ to be equal, they must have the same value for each positive integer, and so each decimal digit of x_1 must equal the corresponding decimal digit of x_2, which implies that $x_1 = x_2$. Thus F is a one-to-one correspondence from S to a subset of T. But S is uncountable by Theorem 7.4.2. Hence T has an uncountable subset, and so, by Corollary 7.4.4, T is uncountable.

b. Part (a) shows that the set T of all functions from $\mathbf{Z}^+$ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is uncountable. But, by Example 7.4.6, given any computer language, the set of all programs in that language is countable. Consequently, in any computer language there are not enough programs to compute values of every function in T. There must exist functions that are not computable! ■

TEST YOURSELF

1. A set is finite if, and only if, _____.
2. To prove that a set A has the same cardinality as a set B you must _____.
3. The reflexive property of cardinality says that given any set A, _____.
4. The symmetric property of cardinality says that given any sets A and B, _____.
5. The transitive property of cardinality says that given any sets A, B, and C, _____.
6. A set is called countably infinite if, and only if, _____.
7. A set is called countable if, and only if, _____.
8. In each of the following, fill in the blank with the word *countable* or the word *uncountable*.
   (a) The set of all integers is _____.
   (b) The set of all rational numbers is _____.
   (c) The set of all real numbers between 0 and 1 is _____.
   (d) The set of all real numbers is _____.
9. The Cantor diagonalization process is used to prove that _____.

EXERCISE SET 7.4

1. When asked what it means to say that set A has the same cardinality as set B, a student replies, "A and B are one-to-one and onto." What *should* the student have replied? Why?
2. Show that "there are as many squares as there are numbers" by exhibiting a one-to-one correspondence from the positive integers, $\mathbf{Z}^+$, to the set S of all squares of positive integers:

   $S = \{n \in \mathbf{Z}^+ \mid n = k^2, \text{ for some positive integer } k\}$.

3. Let $3\mathbf{Z} = \{n \in \mathbf{Z} | n = 3k, \text{ for some integer } k\}$. Prove that $\mathbf{Z}$ and $3\mathbf{Z}$ have the same cardinality.

4. Let $\mathbf{O}$ be the set of all odd integers. Prove that $\mathbf{O}$ has the same cardinality as $2\mathbf{Z}$, the set of all even integers.

5. Let $25\mathbf{Z}$ be the set of all integers that are multiples of 25. Prove that $25\mathbf{Z}$ has the same cardinality as $2\mathbf{Z}$, the set of all even integers.

***H* 6.** Use the functions I and J defined in the paragraph following Example 7.4.1 to show that even though there is a one-to-one correspondence, H, from $2\mathbf{Z}$ to $\mathbf{Z}$, there is also a function from $2\mathbf{Z}$ to $\mathbf{Z}$ that is one-to-one but not onto and a function from $\mathbf{Z}$ to $2\mathbf{Z}$ that is onto but not one-to-one. In other words, show that I is one-to-one but not onto, and show that J is onto but not one-to-one.

7. a. Check that the formula for F given at the end of Example 7.4.2 produces the correct values for $n = 1, 2, 3$, and 4.

b. Use the floor function to write a formula for F as a single algebraic expression for each positive integer n.

8. Use the result of exercise 3 to prove that $3\mathbf{Z}$ is countable.

9. Show that the set of all nonnegative integers is countable by exhibiting a one-to-one correspondence between $\mathbf{Z}^+$ and $\mathbf{Z}^{nonneg}$.

In 10–14 S denotes the set of real numbers strictly between 0 and 1. That is, $S = \{x \in \mathbf{R} | 0 < x < 1\}$.

10. Let $U = \{x \in \mathbf{R} | 0 < x < 2\}$. Prove that S and U have the same cardinality.

***H* 11.** Let $V = \{x \in \mathbf{R} | 2 < x < 5\}$. Prove that S and V have the same cardinality.

12. Let a and b be real numbers with $a < b$, and suppose that $W = \{x \in \mathbf{R} | a < x < b\}$. Prove that S and W have the same cardinality.

13. Draw the graph of the function f defined by the following formula:
For each real number x with $0 < x < 1$,

$$f(x) = \tan\left(\pi x - \frac{\pi}{2}\right).$$

Use the graph to explain why S and $\mathbf{R}$ have the same cardinality.

***** 14.** Define a function g from the set of real numbers to S by the following formula:
For each real number x,

$$g(x) = \frac{1}{2} \cdot \left(\frac{x}{1 + |x|}\right) + \frac{1}{2}.$$

Prove that g is a one-to-one correspondence. (It is possible to prove this statement either with calculus or without it.) What conclusion can you draw from this fact?

15. Show that the set of all bit strings (strings of 0's and 1's) is countable.

16. Show that $\mathbf{Q}$, the set of all rational numbers, is countable.

***H* 17.** Show that $\mathbf{Q}$, the set of all rational numbers, is dense along the number line by showing that given any two rational numbers r_1 and r_2 with $r_1 < r_2$, there exists a rational number x such that $r_1 < x < r_2$.

***H* 18.** Must the average of two irrational numbers always be irrational? Prove or give a counterexample.

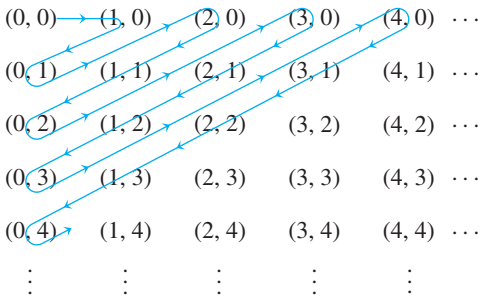
***H*19.** Show that the set of all irrational numbers is dense along the number line by showing that given any two real numbers, there is an irrational number in between.

20. Give two examples of functions from $\mathbf{Z}$ to $\mathbf{Z}$ that are one-to-one but not onto.

21. Give two examples of functions from $\mathbf{Z}$ to $\mathbf{Z}$ that are onto but not one-to-one.

***H* 22.** Define a function g: $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ by the formula $g(m, n) = 2^m 3^n$ for all $(m, n) \in \mathbf{Z}^+ \times \mathbf{Z}^+$. Show that g is one-to-one and use this result to prove that $\mathbf{Z}^+ \times \mathbf{Z}^+$ is countable.

23. a. Explain how to use the following diagram to show that $\mathbf{Z}^{nonneg} \times \mathbf{Z}^{nonneg}$ and $\mathbf{Z}^{nonneg}$ have the same cardinality.



H **b.** Define a function H: $\mathbf{Z}^{nonneg} \times \mathbf{Z}^{nonneg} \to \mathbf{Z}^{nonneg}$ by the formula

$$H(m, n) = n + \frac{(m + n)(m + n + 1)}{2}$$

for all nonnegative integers m and n. Interpret the action of H geometrically using the diagram of part (a).

* **24.** Prove that the function H defined analytically in exercise 23b is a one-to-one correspondence.

H **25.** Prove that $0.1999\ldots = 0.2$.

26. Prove that any infinite set contains a countably infinite subset.

27. Prove that if A is any countably infinite set, B is any set, and $g: A \longrightarrow B$ is onto, then B is countable.

28. Prove that a disjoint union of any finite set and any countably infinite set is countably infinite.

H **29.** Prove that a union of any two countably infinite sets is countably infinite.

H **30.** Use the result of exercise 29 to prove that the set of all irrational numbers is uncountable.

H **31.** Use the results of exercises 28 and 29 to prove that a union of any two countable sets is countable.

H **32.** Prove that $\mathbf{Z} \times \mathbf{Z}$, the Cartesian product of the set of integers with itself, is countably infinite.

33. Use the results of exercises 27, 31, and 32 to prove the following: If R is the set of all solutions to all equations of the form $x^2 + bx + c = 0$, where b and c are integers, then R is countable.

H **34.** Let $\mathcal{P}(S)$ be the set of all subsets of set S, and let T be the set of all functions from S to $\{0, 1\}$. Show that $\mathcal{P}(S)$ and T have the same cardinality.

H **35.** Let S be a set and let $\mathcal{P}(S)$ be the set of all subsets of S. Show that S is "smaller than" $\mathcal{P}(S)$ in the sense that there is a one-to-one function from S to $\mathcal{P}(S)$ but there is no onto function from S to $\mathcal{P}(S)$.

* **36.** The Schroeder–Bernstein theorem states the following: If A and B are any sets with the property that there is a one-to-one function from A to B and a one-to-one function from B to A, then A and B have the same cardinality. Use this theorem to prove that there are as many functions from $\mathbf{Z}^+$ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ as there are functions from $\mathbf{Z}^+$ to $\{0, 1\}$.

H **37.** Prove that if A and B are any countably infinite sets, then $A \times B$ is countably infinite.

* **38.** Suppose $A_1, A_2, A_3, \ldots$ is an infinite sequence of countable sets. Recall that

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ for some positive integer } i\}.$$

Prove that $\bigcup_{i=1}^{\infty} A_i$ is countable. (In other words, prove that a countably infinite union of countable sets is countable.)

ANSWERS FOR TEST YOURSELF

1. it is the empty set or there is a one-to-one correspondence from $\{1, 2, \ldots, n\}$ to it, where n is a positive integer **2.** show that there exists a function from A to B that is one-to-one and onto (*Or:* show that there exists a one-to-one correspondence from A to B) **3.** A has the same cardinality as A **4.** if A has the same cardinality as B, then B has the same cardinality as A **5.** if A has the same cardinality as B and B has the same cardinality as C, then A has the same cardinality as C **6.** it has the same cardinality as the set of all positive integers **7.** it is finite or countably infinite **8.** countable; countable; uncountable; uncountable **9.** the set of all real numbers between 0 and 1 is uncountable

CHAPTER 8 PROPERTIES OF RELATIONS

In this chapter we discuss the mathematics of relations defined on sets, focusing on ways to represent relations and exploring various properties they may have. The concept of equivalence relation is introduced in Section 8.3 and applied in Section 8.4 to modular arithmetic and cryptography. Partial order relations are discussed in Section 8.5, and an application is given showing how to use these relations to help coordinate and guide the flow of individual tasks that must be performed to accomplish a complex, large-scale project.

8.1 Relations on Sets

Strange as it may sound, the power of mathematics rests on its evasion of all unnecessary thought and on its wonderful saving of mental operations. —Ernst Mach, 1838–1916

A more formal way to refer to the kind of relation defined in Section 1.3 is to call it a **binary relation** because it is a subset of a Cartesian product of two sets. At the end of this section we define an *n-ary relation* to be a subset of a Cartesian product of n sets, where n is any integer greater than or equal to two. Such a relation is the fundamental structure used in relational databases. However, because we focus on binary relations in this text, when we use the term *relation* by itself, we will mean binary relation.

Example 8.1.1 **The Less-than Relation for Real Numbers**

Define a relation L from $\mathbf{R}$ to $\mathbf{R}$ as follows: For all real numbers x and y,

$$x \, L \, y \Leftrightarrow x < y.$$

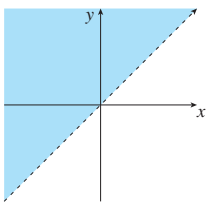
a. Is $57 \, L \, 53$? b. Is $(-17) \, L \, (-14)$? c. Is $143 \, L \, 143$? d. Is $(-35) \, L \, 1$?

e. Draw the graph of L as a subset of the Cartesian plane $\mathbf{R} \times \mathbf{R}$.

Solution

a. No, $57 > 53$. b. Yes, $-17 < -14$. c. No, $143 = 143$. d. Yes, $-35 < 1$.

e. For each value of x, all the points (x, y) with $y > x$ are on the graph. So the graph consists of all the points above the line $x = y$.



■

Example 8.1.2 **The Congruence Modulo 2 Relation**

Define a relation E from $\mathbf{Z}$ to $\mathbf{Z}$ as follows: For every $(m, n) \in \mathbf{Z} \times \mathbf{Z}$,

$$m \, E \, n \quad \Leftrightarrow \quad m - n \text{ is even.}$$

a. Is $4 \, E \, 0$? Is $2 \, E \, 6$? Is $3 \, E \, (-3)$? Is $5 \, E \, 2$?

b. List five integers that are related by E to 1.

c. Prove that if n is any odd integer, then $n \, E \, 1$.

Solution

a. Yes, $4 \, E \, 0$ because $4 - 0 = 4$ and 4 is even.
Yes, $2 \, E \, 6$ because $2 - 6 = -4$ and -4 is even.
Yes, $3 \, E \, (-3)$ because $3 - (-3) = 6$ and 6 is even.
No, $5 \not E \, 2$ because $5 - 2 = 3$ and 3 is not even.

b. There are many such lists. One is

$$\begin{aligned} 1 &\quad \text{because } 1 - 1 = 0 \text{ is even.} \\ 3 &\quad \text{because } 3 - 1 = 2 \text{ is even.} \\ 5 &\quad \text{because } 5 - 1 = 4 \text{ is even.} \\ -1 &\quad \text{because } -1 - 1 = -2 \text{ is even.} \\ -3 &\quad \text{because } -3 - 1 = -4 \text{ is even.} \end{aligned}$$

c. **Proof:** Suppose n is any odd integer. Then $n = 2k + 1$ for some integer k. Now by definition of E, $n \, E \, 1$ if, and only if, $n - 1$ is even. But by substitution,

$$n - 1 = (2k + 1) - 1 = 2k,$$

and since k is an integer, $2k$ is even. Hence $n \, E \, 1$ *[as was to be shown].*

It can be shown (see exercise 2 at the end of this section) that integers m and n are related by E if, and only if, $m \bmod 2 = n \bmod 2$ (that is, both are even or both are odd). When this occurs m and n are said to be **congruent modulo 2**. ■

Example 8.1.3 **A Relation on a Power Set**

Let $X = \{a, b, c\}$. Then $\mathcal{P}(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Define a relation $\mathbf{S}$ from $\mathcal{P}(X)$ to $\mathcal{P}(X)$ as follows: For all sets A and B in $\mathcal{P}(X)$ (that is, for all subsets A and B of X),

$$A \, \mathbf{S} \, B \Leftrightarrow A \text{ has at least as many elements as } B.$$

a. Is $\{a, b\} \, \mathbf{S} \, \{b, c\}$? b. Is $\{a\} \, \mathbf{S} \, \varnothing$? c. Is $\{b, c\} \, \mathbf{S} \, \{a, b, c\}$? d. Is $\{c\} \, \mathbf{S} \, \{a\}$?

Solution

a. Yes, both sets have two elements.

b. Yes, $\{a\}$ has one element and $\varnothing$ has zero elements, and $1 \geq 0$.

c. No, $\{b, c\}$ has two elements and $\{a, b, c\}$ has three elements and $2 < 3$.

d. Yes, both sets have one element. ■

The Inverse of a Relation

If R is a relation from A to B, then a relation R^{-1} from B to A can be defined by interchanging the elements of all the ordered pairs of R.

Definition

Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as follows:

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}.$$

This definition can be written operationally as follows:

For all $x \in A$ and $y \in B$, $\quad (y, x) \in R^{-1} \quad \Leftrightarrow \quad (x, y) \in R.$

Example 8.1.4 **The Inverse of a Finite Relation**

Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$, and let R be the "divides" relation from A to B: For every ordered pair $(x, y) \in A \times B$,

$$x \, R \, y \quad \Leftrightarrow \quad x \mid y \quad x \text{ divides } y.$$

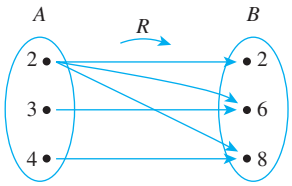
a. State explicitly which ordered pairs are in R and R^{-1}, and draw arrow diagrams for R and R^{-1}.

b. Describe R^{-1} in words.

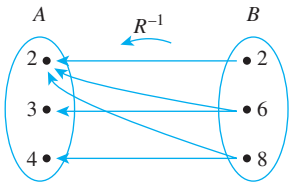
Solution

a. $R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$

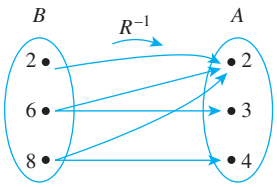
$R^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}$



To draw the arrow diagram for R^{-1}, you can copy the arrow diagram for R but reverse the directions of the arrows.



Or you can redraw the diagram so that B is on the left.



b. R^{-1} can be described in words as follows: For every ordered pair $(y, x) \in B \times A$,

$$y \, R^{-1} x \quad \Leftrightarrow \quad y \text{ is a multiple of } x.$$

■

Example 8.1.5 **The Inverse of an Infinite Relation**

Define a relation R from $\mathbf{R}$ to $\mathbf{R}$ as follows: For every ordered pair $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$x\,R\,y \quad \Leftrightarrow \quad y = 2|x|.$$

Draw the graphs of R and R^{-1} in the Cartesian plane. Is R^{-1} a function?

Solution A point (v, u) is on the graph of R^{-1} if, and only if, (u, v) is on the graph of R. Note that if $x \geq 0$, then the graph of $y = 2|x| = 2x$ is a straight line with slope 2. And if $x < 0$, then the graph of $y = 2|x| = 2(-x) = -2x$ is a straight line with slope -2. Some sample values are tabulated and the graphs are shown below.

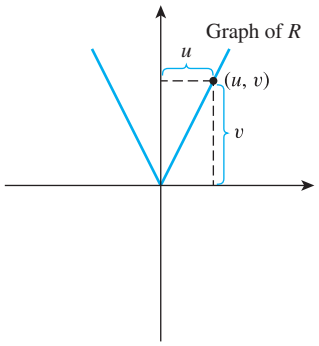
$$R = \{(x, y) | y = 2|x|\} \qquad R^{-1} = \{(y, x) | y = 2|x|\}$$

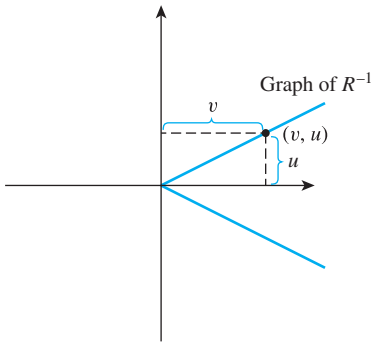
x	y
0	0
1	2
-1	2
2	4
-2	4

1st coordinate 2nd coordinate

y	x
0	0
2	1
2	-1
4	2
4	-2

1st coordinate 2nd coordinate





R^{-1} is not a function because, for instance, both (2, 1) and (2, -1) are in R^{-1}. ■

Directed Graph of a Relation

In the remaining sections of this chapter, we discuss important properties of relations that are defined from a set to itself.

Note Be careful to distinguish clearly between a relation and the set on which it is defined.

Definition

A **relation on a set** A is a relation from A to A.

When a relation R is defined *on* a set A, the arrow diagram of the relation can be modified so that it becomes a **directed graph**. Instead of representing A as two separate sets of points, represent A only once, and draw an arrow from each point of A to each related point. As with an ordinary arrow diagram,

For all points x and y in A,

$$\text{there is an arrow from } x \text{ to } y \quad \Leftrightarrow \quad x\,R\,y \quad \Leftrightarrow \quad (x, y) \in R.$$

If a point is related to itself, a loop is drawn that extends out from the point and goes back to it.

Example 8.1.6 **Directed Graph of a Relation**

Note Read "For every $x, y \in A$" as "For every x and y in A."

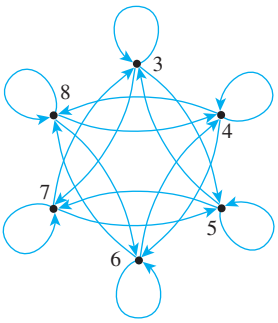
Let $A = \{3, 4, 5, 6, 7, 8\}$ and define a relation R on A as follows: For every $x, y \in A$,

$$x\,R\,y \quad \Leftrightarrow \quad 2 \mid (x - y).$$

Draw the directed graph of R.

Solution Note that $3\,R\,3$ because $3 - 3 = 0$ and $2 \mid 0$ since $0 = 2 \cdot 0$. Thus there is a loop from 3 to itself. Similarly, there is a loop from 4 to itself, from 5 to itself, and so forth, since the difference of each integer with itself is 0, and $2 \mid 0$.

Note also that $3\,R\,5$ because $3 - 5 = -2 = 2 \cdot (-1)$. And $5\,R\,3$ because $5 - 3 = 2 = 2 \cdot 1$. Hence there is an arrow from 3 to 5 and also an arrow from 5 to 3. The other arrows in the directed graph, as shown below, are obtained by similar reasoning.



■

N-*ary Relations and Relational Databases*

A special group of relations, called n-ary relations, form the mathematical foundation for relational database theory. Just as a binary relation is a subset of a Cartesian product of two sets, an n-ary relation is a subset of a Cartesian product of n sets.

Definition

Given sets $A_1, A_2, \ldots, A_n$, an ***n*-ary relation** R on $A_1 \times A_2 \times \cdots \times A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$. The special cases of 2-ary, 3-ary, and 4-ary relations are called **binary, ternary**, and **quaternary relations**, respectively.

Example 8.1.7 **A Simple Database**

The following is a radically simplified version of a database that might be used in a hospital. Let A_1 be a set of positive integers, A_2 a set of alphabetic character strings, A_3 a set of numeric character strings, and A_4 a set of alphabetic character strings. Define a quaternary relation R on $A_1 \times A_2 \times A_3 \times A_4$ as follows:

$$(a_1, a_2, a_3, a_4) \in R \quad \Leftrightarrow \quad \text{a patient with patient ID number } a_1, \text{ named } a_2, \text{ was admitted on date } a_3, \text{ with primary diagnosis } a_4.$$

At a particular hospital, this relation might contain the following 4-tuples:

(011985, John Schmidt, 020719, asthma)

(574329, Tak Kurosawa, 011419, pneumonia)

(466581, Mary Lazars, 010319, appendicitis)

(008352, Joan Kaplan, 112419, gastritis)

(011985, John Schmidt, 021719, pneumonia)

(244388, Sarah Wu, 010319, broken leg)

(778400, Jamal Baskers, 122719, appendicitis)

In discussions of relational databases, the n-tuples are normally thought of as being written in tables. Each row of the table corresponds to one n-tuple, and the header for each column gives the descriptive attribute for the elements in the column.

Operations within a database allow the data to be manipulated in many different ways. For example, in the database language SQL, if the above database is denoted S, the result of the query

SELECT Patient_ID#, Name FROM S WHERE

Admission_Date = 010319

would be a list of the ID numbers and names of all patients admitted on 01-03-19:

466581 Mary Lazars

244388 Sarah Wu

This is obtained by taking the intersection of the set $A_1 \times A_2 \times \{010319\} \times A_4$ with the database and then projecting onto the first two coordinates. (See exercise 25 of Section 7.1.) Similarly, SELECT can be used to obtain a list of all admission dates of a given patient. For John Schmidt this list is

02–07–19

02–17–19

Individual entries in a database can be added, deleted, or updated, and most databases can sort data entries in various ways. In addition, entire databases can be merged, and the entries common to two databases can be moved to a new database. ■

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. If R is a relation from A to B, $x \in A$, and $y \in B$, the notation $x\ R\ y$ means that _____.
2. If R is a relation from A to B, $x \in A$, and $y \in B$, the notation $x \not R\ y$ means that _____.
3. If R is a relation from A to B, $x \in A$, and $y \in B$, then $(y, x) \in R^{-1}$ if, and only if, _____.
4. A relation on a set A is a relation from _____ to _____.
5. If R is a relation on a set A, the directed graph of R has an arrow from x to y if, and only if, _____.

EXERCISE SET 8.1*

1. As in Example 8.1.2, the **congruence modulo 2** relation E is defined from $\mathbf{Z}$ to $\mathbf{Z}$ as follows: For every ordered pair $(m, n) \in \mathbf{Z} \times \mathbf{Z}$,

$$m \, E \, n \quad \Leftrightarrow \quad m - n \text{ is even.}$$

a. Is $0 \, E \, 0$? Is $5 \, E \, 2$? Is $(6, 6) \in E$? Is $(-1, 7) \in E$?
b. Prove that for any even integer n, $n \, E \, 0$.

H 2. Prove that for all integers m and n, $m - n$ is even if, and only if, both m and n are even or both m and n are odd.

3. The **congruence modulo 3** relation, T, is defined from $\mathbf{Z}$ to $\mathbf{Z}$ as follows: For all integers m and n,

$$m \, T \, n \quad \Leftrightarrow \quad 3 \mid (m - n).$$

a. Is $10 \, T \, 1$? Is $1 \, T \, 10$? Is $(2, 2) \in T$? Is $(8, 1) \in T$?
b. List five integers n such that $n \, T \, 0$.
c. List five integers n such that $n \, T \, 1$.
d. List five integers n such that $n \, T \, 2$.
H e. Make and prove a conjecture about which integers are related by T to 0, which integers are related by T to 1, and which integers are related by T to 2.

4. Define a relation P on $\mathbf{Z}$ as follows: For every ordered pair $(m, n) \in \mathbf{Z} \times \mathbf{Z}$,

$$m \, P \, n \Leftrightarrow m \text{ and } n \text{ have a common prime factor.}$$

a. Is $15 \, P \, 25$? **b.** Is $22 \, P \, 27$?
c. Is $0 \, P \, 5$? **d.** Is $8 \, P \, 8$?

5. Let $X = \{a, b, c\}$. Recall that $\mathcal{P}(X)$ is the power set of X. Define a relation $\mathbf{S}$ on $\mathcal{P}(X)$ as follows: For all sets A and B in $\mathcal{P}(X)$,

$$A \, \mathbf{S} \, B \Leftrightarrow A \text{ has the same number of elements as } B.$$

a. Is $\{a, b\} \, \mathbf{S} \, \{b, c\}$? **b.** Is $\{a\} \, \mathbf{S} \, \{a, b\}$?
c. Is $\{c\} \, \mathbf{S} \, \{b\}$?

6. Let $X = \{a, b, c\}$. Define a relation $\mathbf{J}$ on $\mathcal{P}(X)$ as follows: For all sets A and B in $\mathcal{P}(X)$,

$$A \, \mathbf{J} \, B \quad \Leftrightarrow \quad A \cap B \neq \varnothing.$$

a. Is $\{a\} \, \mathbf{J} \, \{c\}$? **b.** Is $\{a, b\} \, \mathbf{J} \, \{b, c\}$?
c. Is $\{a, b\} \, \mathbf{J} \, \{a, b, c\}$?

7. Define a relation R on $\mathbf{Z}$ as follows: For all integers m and n,

$$m \, R \, n \quad \Leftrightarrow \quad 5 \mid (m^2 - n^2).$$

a. Is $1 \, R \, (-9)$? **b.** Is $2 \, R \, 13$?
c. Is $2 \, R \, (-8)$? **d.** Is $(-8) \, R \, 2$?

8. Let A be the set of all strings of a's and b's of length 4. Define a relation R on A as follows: For every $s, t \in A$,

$$s \, R \, t \Leftrightarrow s \text{ has the same first two characters as } t.$$

a. Is $abaa \, R \, abba$? **b.** Is $aabb \, R \, bbaa$?
c. Is $aaaa \, R \, aaab$? **d.** Is $baaa \, R \, abaa$?

9. Let A be the set of all strings of 0's, 1's, and 2's of length 4. Define a relation R on A as follows: For every $s, t \in A$,

$$s \, R \, t \Leftrightarrow \text{the sum of the characters in } s \text{ equals the sum of the characters in } t.$$

a. Is $0121 \, R \, 2200$? **b.** Is $1011 \, R \, 2101$?
c. Is $2212 \, R \, 2121$? **d.** Is $1220 \, R \, 2111$?

10. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and let R be the "less than" relation. That is, for every ordered pair $(x, y) \in A \times B$,

$$x \, R \, y \quad \Leftrightarrow \quad x < y.$$

State explicitly which ordered pairs are in R and R^{-1}.

11. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and let S be the "divides" relation. That is, for every ordered pair $(x, y) \in A \times B$,

$$x \, S \, y \quad \Leftrightarrow \quad x \mid y.$$

State explicitly which ordered pairs are in S and S^{-1}.

12. a. Suppose a function $F: X \to Y$ is one-to-one but not onto. Is F^{-1} (the inverse relation for F) a function? Explain your answer.
b. Suppose a function $F: X \to Y$ is onto but not one-to-one. Is F^{-1} (the inverse relation for F) a function? Explain your answer.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol *H* indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

Draw the directed graphs of the relations defined in 13–18.

13. Define a relation R on $A = \{0, 1, 2, 3\}$ by $R = \{(0, 0), (1, 2), (2, 2)\}$.

14. Define a relation S on $B = \{a, b, c, d\}$ by $S = \{(a, b), (a, c), (b, c), (d, d)\}$.

15. Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation R on A as follows: For every $x, y \in A$,

$$x \, R \, y \quad \Leftrightarrow \quad x \mid y.$$

H **16.** Let $A = \{5, 6, 7, 8, 9, 10\}$ and define a relation S on A as follows: For every $x, y \in A$,

$$x \, S \, y \quad \Leftrightarrow \quad 2 \mid (x - y).$$

17. Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T on A as follows: For every $x, y \in A$,

$$x \, T \, y \quad \Leftrightarrow \quad 3 \mid (x - y).$$

18. Let $A = \{0, 1, 3, 4, 5, 6\}$ and define a relation V on A as follows: For every $x, y \in A$,

$$x \, V \, y \quad \Leftrightarrow \quad 5 \mid (x^2 - y^2).$$

Exercises 19–20 refer to unions and intersections of relations. Since relations are subsets of Cartesian products, their unions and intersections can be calculated as for any subsets. Given two relations *R* and *S* from *A* to *B*,

$$R \cup S = \{(x, y) \in A \times B \mid (x, y) \in R \text{ or } (x, y) \in S\}$$
$$R \cap S = \{(x, y) \in A \times B \mid (x, y) \in R \text{ and } (x, y) \in S\}.$$

19. Let $A = \{2, 4\}$ and $B = \{6, 8, 10\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B$,

$$x \, R \, y \quad \Leftrightarrow \quad x \mid y \quad \text{and}$$
$$x \, S \, y \quad \Leftrightarrow \quad y - 4 = x.$$

State explicitly which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

20. Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B$,

$$x \, R \, y \quad \Leftrightarrow \quad |x| = |y| \text{ and}$$
$$x \, S \, y \quad \Leftrightarrow \quad x - y \text{ is even.}$$

State explicitly which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

21. Define relations R and S on $\mathbf{R}$ as follows:

$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x < y\} \quad \text{and}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = y\}.$$

That is, R is the "less than" relation and S is the "equals" relation on $\mathbf{R}$. Graph R, S, $R \cup S$, and $R \cap S$ in the Cartesian plane.

22. Define relations R and S on $\mathbf{R}$ as follows:

$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x^2 + y^2 = 4\} \quad \text{and}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = y\}.$$

Graph R, S, $R \cup S$, and $R \cap S$ in the Cartesian plane.

23. Define relations R and S on $\mathbf{R}$ as follows:

$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid y = |x|\} \quad \text{and}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid y = 1\}.$$

Graph R, S, $R \cup S$, and $R \cap S$ in the Cartesian plane.

24. In Example 8.1.7 consider the query SELECT Patient_ID#, Name FROM S WHERE Primary_Diagnosis = X. The response to the query is the projection onto the first two coordinates of the intersection of the database with the set $A_1 \times A_2 \times A_3 \times \{X\}$.

a. Find the result of the query SELECT Patient_ID#, Name FROM S WHERE Primary_Diagnosis = pneumonia.

b. Find the result of the query SELECT Patient_ID#, Name FROM S WHERE Primary_Diagnosis = appendicitis.

ANSWERS FOR TEST YOURSELF

1. x is related to y by R **2.** x is not related to y by R **3.** $(x, y) \in R$ **4.** A; A **5.** x is related to y by R

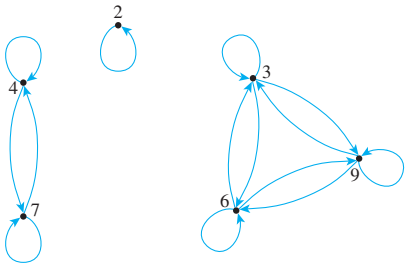
8.2 Reflexivity, Symmetry, and Transitivity

Mathematics is the tool specially suited for dealing with abstract concepts of any kind and there is no limit to its power in this field. —P. A. M. Dirac, 1902–1984

Let $A = \{2, 3, 4, 6, 7, 9\}$ and define a relation R on A as follows: For every $x, y \in A$,

$$x \, R \, y \quad \Leftrightarrow \quad 3 \mid (x - y).$$

Then $2 \, R \, 2$ because $2 - 2 = 0$, and $3 \mid 0$. Similarly, $3 \, R \, 3$, $4 \, R \, 4$, $6 \, R \, 6$, $7 \, R \, 7$, and $9 \, R \, 9$. Also $6 \, R \, 3$ because $6 - 3 = 3$, and $3 \mid 3$. And $3 \, R \, 6$ because $3 - 6 = -(6 - 3) = -3$, and $3 \mid (-3)$. Similarly, $3 \, R \, 9$, $9 \, R \, 3$, $6 \, R \, 9$, $9 \, R \, 6$, $4 \, R \, 7$, and $7 \, R \, 4$. Thus the directed graph for R has the appearance shown below.



This graph has three important properties:

1. Each point of the graph has an arrow looping around from it and going back to it.
2. In each case where there is an arrow going from one point to a second, there is an arrow going from the second point back to the first.
3. In each case where there is an arrow going from one point to a second and from the second point to a third, there is an arrow going from the first point to the third. That is, there are no "incomplete directed triangles" in the graph.

Properties (1), (2), and (3) correspond to properties of general relations called *reflexivity*, *symmetry*, and *transitivity*.

Caution! The definition of symmetric does not say that x is related to y by R; rather, it states only that **if it happens** that x is related to y, then y must be related to x.

Definition

Let R be a relation on a set A.

1. R is **reflexive** if, and only if, for every $x \in A$, $x \, R \, x$.
2. R is **symmetric** if, and only if, for every $x, y \in A$, if $x \, R \, y$ then $y \, R \, x$.
3. R is **transitive** if, and only if, for every $x, y, z \in A$, if $x \, R \, y$ and $y \, R \, z$ then $x \, R \, z$.

Because of the equivalence of the expressions $x \, R \, y$ and $(x, y) \in R$ for every x and y in A, the reflexive, symmetric, and transitive properties can also be written as follows:

1. R is reflexive $\Leftrightarrow$ for every x in A, $(x, x) \in R$.
2. R is symmetric $\Leftrightarrow$ for every x and y in A, ***if*** $(x, y) \in R$ then $(y, x) \in R$.
3. R is transitive $\Leftrightarrow$ for every x, y, and z in A, ***if*** $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

Caution! The "first," "second," and "third" elements in the informal versions need not all be distinct. This is a disadvantage of informality: It may mask nuances that a formal definition makes clear.

In informal terms, properties (1)–(3) say the following:

1. **Reflexive:** Each element is related to itself.
2. **Symmetric:** If any one element is related to any other element, then the second element is related to the first.
3. **Transitive:** If any one element is related to a second and that second element is related to a third, then the first element is related to the third.

Note that the definitions of reflexivity, symmetry, and transitivity are universal statements. This means that to prove a relation has one of the properties, you use either the method of exhaustion or the method of generalizing from the generic particular.

Now consider what it means for a relation *not* to have one of the properties defined previously. Recall that the negation of a universal statement is existential. Hence if R is a relation on a set A, then

1. R is **not reflexive** $\Leftrightarrow$ there is an element x in A such that $x \not R\, x$ *[that is, such that* $(x, x) \notin R$*]*.
2. R is **not symmetric** $\Leftrightarrow$ there are elements x and y in A such that $x\, R\, y$ but $y \not R\, x$ *[that is, such that* $(x, y) \in R$ *but* $(y, x) \notin R$*]*.
3. R is **not transitive** $\Leftrightarrow$ there are elements x, y, and z in A such that $x\, R\, y$ and $y\, R\, z$ but $x \not R\, z$ *[that is, such that* $(x, y) \in R$ *and* $(y, z) \in R$ *but* $(x, z) \notin R$*]*.

It follows that you can show that a relation does *not* have one of the properties by finding a counterexample.

Example 8.2.1 **Properties of Relations on Finite Sets**

Let $A = \{0, 1, 2, 3\}$ and define relations R, S, and T on A as follows:

$$R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\},$$
$$S = \{(0, 0), (0, 2), (0, 3), (2, 3)\},$$
$$T = \{(0, 1), (2, 3)\}.$$

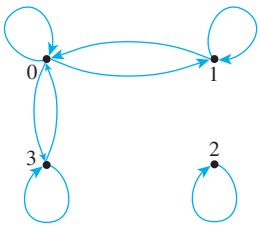
a. Is R reflexive? symmetric? transitive?

b. Is S reflexive? symmetric? transitive?

c. Is T reflexive? symmetric? transitive?

Solution

a. The directed graph of R has the appearance shown below.

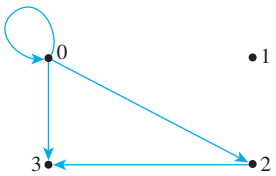


***R is reflexive*:** There is a loop at each point of the directed graph. This means that each element of A is related to itself, so R is reflexive.

***R is symmetric*:** In each case where there is an arrow going from one point of the graph to a second, there is an arrow going from the second point back to the first. This means that whenever one element of A is related by R to a second, then the second is related to the first. Hence R is symmetric.

***R is not transitive*:** There is an arrow going from 1 to 0 and an arrow going from 0 to 3, but there is no arrow going from 1 to 3. This means that there are elements of A—0, 1, and 3—such that $1 \; R \; 0$ and $0 \; R \; 3$ but $1 \not R \; 3$. Hence R is not transitive.

b. The directed graph of S has the appearance shown below.



***S is not reflexive*:** There is no loop at 1, for example. Thus $(1, 1) \notin S$, and so S is not reflexive.

***S is not symmetric*:** There is an arrow from 0 to 2 but not from 2 to 0. Hence $(0, 2) \in S$ but $(2, 0) \notin S$, and so S is not symmetric.

***S is transitive*:** There are three cases for which there is an arrow going from one point of the graph to a second and from the second point to a third. In particular, there are arrows going from 0 to 2 and from 2 to 3; there are arrows going from 0 to 0 and from 0 to 2; and there are arrows going from 0 to 0 and from 0 to 3. In each case there is an arrow going from the first point to the third. (Note again that the "first," "second," and "third" points need not be distinct.) This means that whenever $(x, y) \in S$ and $(y, z) \in S$, then $(x, z) \in S$, for every $x, y, z \in \{0, 1, 2, 3\}$, and so S is transitive.

c. The directed graph of T has the appearance shown below.

***T is not reflexive*:** There is no loop at 0, for example. Thus $(0, 0) \notin T$, so T is not reflexive.

***T is not symmetric*:** There is an arrow from 0 to 1 but not from 1 to 0. Thus $(0, 1) \in T$ but $(1, 0) \notin T$, and so T is not symmetric.

Note *T* is transitive by default because it is *not* not transitive!

***T is transitive*:** The transitivity condition is vacuously true for T. To see this, observe that the transitivity condition says that

$$\text{For every } x, y, z \in A, \quad \text{if } (x, y) \in T \text{ and } (y, z) \in T \text{ then } (x, z) \in T.$$

The only way for this to be false would be for there to exist elements of A that make the hypothesis true and the conclusion false. That is, there would have to be elements x, y, and z in A such that

$$(x, y) \in T \quad \text{and} \quad (y, z) \in T \quad \text{and} \quad (x, z) \notin T.$$

In other words, there would have to be two ordered pairs in T that have the potential to "link up" by having the *second* element of one pair be the *first* element of the other pair. But the only elements in T are (0, 1) and (2, 3), and these do not have the potential to link up. Hence the hypothesis is never true. It follows that it is impossible for T *not* to be transitive, and thus T is transitive. ■

When a relation R is defined on a finite set A, it is possible to write computer algorithms to check whether R is reflexive, symmetric, and transitive. One way to do this is to represent A as a one-dimensional array, $(a[1], a[2], \ldots, a[n])$ and use a modification of the algorithm of exercise 38 in Section 6.1 to check whether an ordered pair in $A \times A$ is in R. Checking whether R is reflexive can be done with a loop that examines each element $a[i]$ of A in turn. If, for some i, $(a[i], a[i]) \notin R$, then R is not reflexive. Otherwise, R is reflexive. Checking for symmetry can be done with a nested loop that examines each pair $(a[i], a[j])$ of $A \times A$ in turn. If, for some i and j, $(a[i], a[j]) \in R$ and $(a[j], a[i]) \notin R$, then R is not symmetric. Otherwise, R is symmetric. Checking whether R is transitive can be done with a triply nested loop that examines each triple $(a[i], a[j], a[k])$ of $A \times A \times A$ in turn. If, for some triple, $(a[i], a[j]) \in R$, $(a[j], a[k]) \in R$, and $(a[i], a[k]) \notin R$, then R is not transitive. Otherwise, R is transitive. In the exercises for this section, you are asked to formalize these algorithms.

Properties of Relations on Infinite Sets

Suppose a relation R is defined on an infinite set A. To prove the relation is reflexive, symmetric, or transitive, first write down what is to be proved. For instance, for symmetry you need to prove that

$$\forall x, y \in A, \text{ if } x \, R \, y \text{ then } y \, R \, x.$$

Then use the definitions of A and R to rewrite the statement for the particular case in question. For instance, for the "equality" relation on the set of real numbers, the rewritten statement is

$$\forall x, y \in \mathbf{R}, \text{ if } x = y \text{ then } y = x.$$

Sometimes the truth of the rewritten statement will be immediately obvious (as it is here). At other times you will need to prove it using the method of generalizing from the generic particular. We give examples of both cases in this section. We begin with the relation of equality, one of the simplest and yet most important relations.

Example 8.2.2 **Properties of Equality**

Define a relation R on $\mathbf{R}$ as follows: For all real numbers x and y,

$$x \, R \, y \quad \Leftrightarrow \quad x = y.$$

a. Is R reflexive? b. Is R symmetric? c. Is R transitive?

Solution

a. ***R is reflexive*:** R is reflexive if, and only if, the following statement is true:

$$\text{For every } x \in \mathbf{R}, \quad x \, R \, x.$$

Since $x \, R \, x$ just means that $x = x$, this is the same as saying

$$\text{For every } x \in \mathbf{R}, \quad x = x.$$

But this statement is certainly true; every real number is equal to itself.

b. ***R is symmetric*:** R is symmetric if, and only if, the following statement is true:

$$\text{For every } x, y \in \mathbf{R}, \quad \text{if } x \, R \, y \text{ then } y \, R \, x.$$

By definition of R, $x\ R\ y$ means that $x = y$ and $y\ R\ x$ means that $y = x$. Hence R is symmetric if, and only if,

$$\text{For every } x, y \in \mathbf{R}, \quad \textbf{if } x = y \text{ then } y = x.$$

But this statement is certainly true; if one number is equal to a second, then the second is equal to the first.

c. ***R is transitive*:** R is transitive if, and only if, the following statement is true:

$$\text{For every } x, y, z \in \mathbf{R}, \quad \textbf{if } x\ R\ y \text{ and } y\ R\ z \text{ then } x\ R\ z.$$

By definition of R, $x\ R\ y$ means that $x = y$, $y\ R\ z$ means that $y = z$, and $x\ R\ z$ means that $x = z$. Hence R is transitive if, and only if, the following statement is true:

$$\text{For every } x, y, z \in \mathbf{R}, \quad \textbf{if } x = y \text{ and } y = z \text{ then } x = z.$$

But this statement is certainly true: If one real number equals a second and the second equals a third, then the first equals the third. ■

Example 8.2.3 **Properties of "Less Than"**

Define a relation R on $\mathbf{R}$ as follows: For all real numbers x and y,

$$x\ R\ y \quad \Leftrightarrow \quad x < y.$$

a. Is R reflexive? b. Is R symmetric? c. Is R transitive?

Solution

a. ***R is not reflexive*:** R is reflexive if, and only if, $\forall x \in \mathbf{R}$, $x\ R\ x$. By definition of R, this means that $\forall x \in \mathbf{R}$, $x < x$. But this is false: $\exists x \in \mathbf{R}$ such that $x \not< x$. As a counterexample, let $x = 0$ and note that $0 \not< 0$. Hence R is not reflexive.

b. ***R is not symmetric*:** R is symmetric if, and only if, $\forall x, y \in \mathbf{R}$, if $x\ R\ y$ then $y\ R\ x$. By definition of R, this means that $\forall x, y \in \mathbf{R}$, if $x < y$ then $y < x$. But this is false: $\exists x, y \in \mathbf{R}$ such that $x < y$ and $y \not< x$. As a counterexample, let $x = 0$ and $y = 1$ and note that $0 < 1$ but $1 \not< 0$. Hence R is not symmetric.

c. ***R is transitive*:** R is transitive if, and only if, $\forall x, y, z \in \mathbf{R}$, if $x\ R\ y$ and $y\ R\ z$ then $x\ R\ z$. By definition of R, this means that $\forall x, y, z \in \mathbf{R}$, if $x < y$ and $y < z$, then $x < z$. But this statement is true by the transitive law of order for real numbers (Appendix A, T18). Hence R is transitive. ■

Sometimes a property is "universally false" in the sense that it is false for *every* element of its domain. It follows immediately, of course, that the property is false for each particular element of the domain and hence counterexamples abound. In such a case, it may seem more natural to prove the universal falseness of the property rather than to give a single counterexample. In the example above, for instance, you might find it natural to answer (a) and (b) as follows:

Alternative Answer to (a): R is not reflexive because $x \not< x$ for every real number x (by the trichotomy law—Appendix A, T17).

Alternative Answer to (b): R is not symmetric because for all real numbers x and y in A, if $x < y$ then $y \not< x$ (by the trichotomy law).

Example 8.2.4 **Properties of Congruence Modulo 3**

Define a relation T on $\mathbf{Z}$ (the set of all integers) as follows: For all integers m and n,

$$m\ T\ n \quad \Leftrightarrow \quad 3 \mid (m-n).$$

This relation is called **congruence modulo 3**.

a. Is T reflexive? b. Is T symmetric? c. Is T transitive?

Solution

a. ***T is reflexive*:** To show that T is reflexive, it is necessary to show that

$$\text{For every } m \in \mathbf{Z}, \quad m\ T\ m.$$

By definition of T, this means that

$$\text{For every } m \in \mathbf{Z}, \quad 3 \mid (m-m),$$

which is true because $m-m=0$ and $3 \mid 0$ (since $0 = 3\cdot 0$). Hence T is reflexive. This reasoning is formalized in the following proof.

Proof of Reflexivity: Suppose m is a particular but arbitrarily chosen integer. *[We must show that m T m.]* Now $m-m=0$. But $3 \mid 0$ since $0 = 3\cdot 0$. Hence $3 \mid (m-m)$. Thus, by definition of T, $m\ T\ m$ *[as was to be shown].*

b. ***T is symmetric*:** To show that T is symmetric, it is necessary to show that

$$\text{For every } m, n \in \mathbf{Z}, \quad \textbf{if } m\ T\ n \text{ then } n\ T\ m.$$

By definition of T this means that

$$\text{For every } m, n \in \mathbf{Z}, \quad \textbf{if } 3 \mid (m-n) \text{ then } 3 \mid (n-m).$$

Is this true? Suppose m and n are particular but arbitrarily chosen integers such that $3 \mid (m-n)$. Must it follow that $3 \mid (n-m)$? *[In other words, can we find an integer so that $n-m = 3\cdot$(that integer)?]* By definition of "divides," since

$$3 \mid (m-n),$$

then

$$m-n = 3k \quad \text{for some integer } k.$$

The crucial observation is that $n-m = -(m-n)$. Hence, you can multiply both sides of this equation by -1 to obtain

$$-(m-n) = -3k,$$

which is equivalent to

$$n-m = 3(-k).$$

[Thus we have found an integer, $-k$, so that $n-m = 3\cdot$(that integer).]

Since $-k$ is an integer, this equation shows that

$$3 \mid (n-m).$$

It follows that T is symmetric.

The reasoning above is formalized in the following proof.

Proof of Symmetry: Suppose m and n are particular but arbitrarily chosen integers that satisfy the condition $m\ T\ n$. *[We must show that $n\ T\ m$.]* By definition of T, since $m\ T\ n$ then $3 \mid (m-n)$. By definition of "divides," this means that $m-n = 3k$, for some integer k. Multiplying both sides by -1 gives $n-m = 3(-k)$. Since $-k$ is an integer, this equation shows that $3 \mid (n-m)$. Hence, by definition of T, $n\ T\ m$ *[as was to be shown].*

c. ***T is transitive*:** To show that T is transitive, it is necessary to show that

$$\text{For every } m, n, p \in \mathbf{Z}, \quad \textbf{if } m\ T\ n \text{ and } n\ T\ p \text{ then } m\ T\ p.$$

By definition of T this means that

$$\text{For every } m, n \in \mathbf{Z}, \quad \textbf{if } 3 \mid (m-n) \text{ and } 3 \mid (n-p) \text{ then } 3 \mid (m-p).$$

Is this true? Suppose m, n, and p are particular but arbitrarily chosen integers such that $3 \mid (m-n)$ and $3 \mid (n-p)$. Must it follow that $3 \mid (m-p)$? *[In other words, can we find an integer so that $m-p = 3\cdot$(that integer)?]* By definition of "divides," since

$$3 \mid (m-n) \quad \text{and} \quad 3 \mid (n-p),$$

then

$$m-n = 3r \quad \text{for some integer } r,$$

and

$$n-p = 3s \quad \text{for some integer } s.$$

The crucial observation is that $(m-n)+(n-p) = m-p$. Add these two equations together to obtain

$$(m-n)+(n-p) = 3r+3s,$$

which is equivalent to

$$m-p = 3(r+s).$$

[Thus we have found an integer so that $m-p = 3\cdot$(that integer).] Since r and s are integers, $r+s$ is an integer. So this equation shows that

$$3 \mid (m-p).$$

It follows that T is transitive.

The reasoning above is formalized in the following proof.

Proof of Transitivity: Suppose m, n, and p are particular but arbitrarily chosen integers that satisfy the condition $m\ T\ n$ and $n\ T\ p$. *[We must show that $m\ T\ p$.]* By definition of T, since $m\ T\ n$ and $n\ T\ p$, then $3 \mid (m-n)$ and $3 \mid (n-p)$. By definition of "divides," this means that $m-n = 3r$ and $n-p = 3s$, for some integers r and s. Adding the two equations gives $(m-n)+(n-p) = 3r+3s$, and simplifying gives that $m-p = 3(r+s)$. Since $r+s$ is an integer, this equation shows that $3 \mid (m-p)$. Hence, by definition of T, $m\ T\ p$ *[as was to be shown].*

■

The Transitive Closure of a Relation

Generally speaking, a relation fails to be transitive because it fails to contain certain ordered pairs. For example, if (1, 3) and (3, 4) are in a relation R, then the pair (1, 4) *must* be in R if R is to be transitive. To obtain a transitive relation from one that is not transitive, it is necessary to add ordered pairs. Roughly speaking, the relation obtained by adding the least number of ordered pairs to ensure transitivity is called the *transitive closure* of the relation. More precisely, the transitive closure of a relation is the smallest transitive relation that contains the relation.

Definition

Let A be a set and R a relation on A. The **transitive closure** of R is the relation R^t on A that satisfies the following three properties:

1. R^t is transitive.
2. $R \subseteq R^t$.
3. If S is any other transitive relation that contains R, then $R^t \subseteq S$.

Example 8.2.5 **Transitive Closure of a Relation**

Let $A = \{0, 1, 2, 3\}$ and consider the relation R defined on A as follows:

$$R = \{(0, 1), (1, 2), (2, 3)\}.$$

Find the transitive closure of R.

Solution Every ordered pair in R is in R^t, so

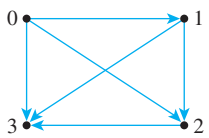
$$\{(0, 1), (1, 2), (2, 3)\} \subseteq R^t.$$

Thus the directed graph of R contains the arrows shown below.

Since there are arrows going from 0 to 1 and from 1 to 2, R^t must have an arrow going from 0 to 2. Hence $(0, 2) \in R^t$. Then $(0, 2) \in R^t$ and $(2, 3) \in R^t$, so since R^t is transitive, $(0, 3) \in R^t$. Also, since $(1, 2) \in R^t$ and $(2, 3) \in R^t$, then $(1, 3) \in R^t$. Thus R^t contains at least the following ordered pairs:

$$\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}.$$

But this relation *is* transitive; hence it equals R^t. The directed graph of R^t is shown below.



■

TEST YOURSELF

1. For a relation R on a set A to be reflexive means that _____.
2. For a relation R on a set A to be symmetric means that _____.
3. For a relation R on a set A to be transitive means that _____.
4. To show that a relation R on an infinite set A is reflexive, you suppose that _____ and you show that _____.
5. To show that a relation R on an infinite set A is symmetric, you suppose that _____ and you show that _____.
6. To show that a relation R on an infinite set A is transitive, you suppose that _____ and you show that _____.
7. To show that a relation R on a set A is not reflexive, you _____.
8. To show that a relation R on a set A is not symmetric, you _____.
9. To show that a relation R on a set A is not transitive, you _____.
10. Given a relation R on a set A, the transitive closure of R is the relation R^t on A that satisfies the following three properties: _____, _____, and _____.

EXERCISE SET 8.2

In 1–8, a number of relations are defined on the set $A = \{0, 1, 2, 3\}$. For each relation:

a. Draw the directed graph.
b. Determine whether the relation is reflexive.
c. Determine whether the relation is symmetric.
d. Determine whether the relation is transitive.

Give a counterexample in each case in which the relation does not satisfy one of the properties.

1. $R_1 = \{(0, 0), (0, 1), (0, 3), (1, 1), (1, 0), (2, 3), (3, 3)\}$
2. $R_2 = \{(0, 0), (0, 1), (1, 1), (1, 2), (2, 2), (2, 3)\}$
3. $R_3 = \{(2, 3), (3, 2)\}$
4. $R_4 = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$
5. $R_5 = \{(0, 0), (0, 1), (0, 2), (1, 2)\}$
6. $R_6 = \{(0, 1), (0, 2)\}$
7. $R_7 = \{(0, 3), (2, 3)\}$
8. $R_8 = \{(0, 0), (1, 1)\}$

In 9–33, determine whether the given relation is reflexive, symmetric, transitive, or none of these. Justify your answers.

9. R is the "greater than or equal to" relation on the set of real numbers: For every $x, y \in \mathbf{R}$, $x \, R \, y \Leftrightarrow x \geq y$.
10. C is the circle relation on the set of real numbers: For every $x, y \in \mathbf{R}$, $x \, C \, y \Leftrightarrow x^2 + y^2 = 1$.
11. D is the relation defined on $\mathbf{R}$ as follows: For every $x, y \in \mathbf{R}$, $x \, D \, y \Leftrightarrow xy \geq 0$.
12. E is the congruence modulo 4 relation on $\mathbf{Z}$: For every $m, n \in \mathbf{Z}$, $m \, E \, n \Leftrightarrow 4 \mid (m - n)$.
13. F is the congruence modulo 5 relation on $\mathbf{Z}$: For every $m, n \in \mathbf{Z}$, $m \, F \, n \Leftrightarrow 5 \mid (m - n)$.
14. O is the relation defined on $\mathbf{Z}$ as follows: For every $m, n \in \mathbf{Z}$, $m \, O \, n \Leftrightarrow m - n$ is odd.
15. D is the "divides" relation on $\mathbf{Z}^+$: For all positive integers m and n, $m \, D \, n \Leftrightarrow m \mid n$.
16. A is the "absolute value" relation on $\mathbf{R}$: For all real numbers x and y, $x \, A \, y \Leftrightarrow |x| = |y|$.
17. Recall that a prime number is an integer that is greater than 1 and has no positive integer divisors other than 1 and itself. (In particular, 1 is not prime.) A relation P is defined on $\mathbf{Z}$ as follows: For every $m, n \in \mathbf{Z}$, $m \, P \, n \Leftrightarrow \exists$ a prime number p such that $p \mid m$ and $p \mid n$.

H 18. Define a relation Q on $\mathbf{R}$ as follows: For all real numbers x and y, $x \, Q \, y \Leftrightarrow x - y$ is rational.

19. Define a relation I on $\mathbf{R}$ as follows: For all real numbers x and y, $x \, I \, y \Leftrightarrow x - y$ is irrational.
20. Let $X = \{a, b, c\}$ and $\mathcal{P}(X)$ be the power set of X (the set of all subsets of X). A relation $\mathbf{E}$ is defined on $\mathcal{P}(X)$ as follows: For every $A, B \in \mathcal{P}(X)$, $A \, \mathbf{E} \, B \Leftrightarrow$ the number of elements in A equals the number of elements in B.

21. Let $X = \{a, b, c\}$ and $\mathcal{P}(X)$ be the power set of X. A relation **L** is defined on $\mathcal{P}(X)$ as follows: For every $A, B \in \mathcal{P}(X)$, A **L** $B \Leftrightarrow$ the number of elements in A is less than the number of elements in B.

22. Let $X = \{a, b, c\}$ and $\mathcal{P}(X)$ be the power set of X. A relation **N** is defined on $\mathcal{P}(X)$ as follows: For every $A, B \in \mathcal{P}(X)$, A **N** $B \Leftrightarrow$ the number of elements in A is not equal to the number of elements in B.

23. Let X be a nonempty set and $\mathcal{P}(X)$ the power set of X. Define the "subset" relation **S** on $\mathcal{P}(X)$ as follows: For every $A, B \in \mathcal{P}(X)$, A **S** $B \Leftrightarrow A \subseteq B$.

24. Let X be a nonempty set and $\mathcal{P}(X)$ the power set of X. Define the "not equal to" relation **U** on $\mathcal{P}(X)$ as follows: For every $A, B \in \mathcal{P}(X)$, A **U** $B \Leftrightarrow A \neq B$.

25. Let A be the set of all strings of a's and b's of length 4. Define a relation R on A as follows: For every $s, t \in A$, $s\ R\ t \Leftrightarrow s$ has the same first two characters as t.

26. Let A be the set of all strings of 0's, 1's, and 2's that have length 4 and for which the sum of the characters in the string is less than or equal to 2. Define a relation R on A as follows: For every $s, t \in A$, $s\ R\ t \Leftrightarrow$ the sum of the characters of s equals the sum of the characters of t.

27. Let A be the set of all English statements. A relation **I** is defined on A as follows: For every $p, q \in A$,

$$p\ \mathbf{I}\ q \Leftrightarrow p \rightarrow q \text{ is true.}$$

28. Let $A = \mathbf{R} \times \mathbf{R}$. A relation **F** is defined on A as follows: For every (x_1, y_1) and (x_2, y_2) in A,

$$(x_1, y_1)\ \mathbf{F}\ (x_2, y_2) \Leftrightarrow x_1 = x_2.$$

29. Let $A = \mathbf{R} \times \mathbf{R}$. A relation **S** is defined on A as follows: For every (x_1, y_1) and (x_2, y_2) in A,

$$(x_1, y_1)\ \mathbf{S}\ (x_2, y_2) \Leftrightarrow y_1 = y_2.$$

30. Let A be the "punctured plane"; that is, A is the set of all points in the Cartesian plane except the origin (0, 0). A relation R is defined on A as follows: For every p_1 and p_2 in A, $p_1\ R\ p_2 \Leftrightarrow p_1$ and p_2 lie on the same half line emanating from the origin.

31. Let A be the set of people living in the world today. A relation R is defined on A as follows: For all people p and q in A,

$$p\ R\ q \Leftrightarrow p \text{ lives within 100 miles of } q.$$

32. Let A be the set of all lines in the plane. A relation R is defined on A as follows: For every l_1 and l_2 in A, $l_1\ R\ l_2 \Leftrightarrow l_1$ is parallel to l_2. (Assume that a line is parallel to itself.)

33. Let A be the set of all lines in the plane. A relation R is defined on A as follows: For every l_1 and l_2 in A,

$$l_1\ R\ l_2 \Leftrightarrow l_1 \text{ is perpendicular to } l_2.$$

In 34–36, assume that *R* is a relation on a set *A*. Prove or disprove each statement.

34. If R is reflexive, then R^{-1} is reflexive.

35. If R is symmetric, then R^{-1} is symmetric.

36. If R is transitive, then R^{-1} is transitive.

In 37–42, assume that *R* and *S* are relations on a set *A*. Prove or disprove each statement.

37. If R and S are reflexive, is $R \cap S$ reflexive? Why?

H 38. If R and S are symmetric, is $R \cap S$ symmetric? Why?

39. If R and S are transitive, is $R \cap S$ transitive? Why?

40. If R and S are reflexive, is $R \cup S$ reflexive? Why?

41. If R and S are symmetric, is $R \cup S$ symmetric? Why?

42. If R and S are transitive, is $R \cup S$ transitive? Why?

In 43–50, the following definitions are used: A relation on a set *A* is defined to be

irreflexive if, and only if, for every $x \in A$, $x \not R\ x$;

asymmetric if, and only if, for every $x, y \in A$ if $x\ R\ y$ then $y \not R\ x$;

intransitive if, and only if, for every $x, y, z \in A$, if $x\ R\ y$ and $y\ R\ z$ then $x \not R\ z$.

For each of the relations in the referenced exercise, determine whether the relation is irreflexive, asymmetric, intransitive, or none of these.

43. Exercise 1 **44.** Exercise 2

45. Exercise 3 **46.** Exercise 4

47. Exercise 5 **48.** Exercise 6

49. Exercise 7 **50.** Exercise 8

In 51–53, *R*, *S*, and *T* are relations defined on $A = \{0, 1, 2, 3\}$.

51. Let $R = (0, 1), (0, 2), (1, 1), (1, 3), (2, 2), (3, 0)$. Find R^t, the transitive closure of R.

52. Let $S = \{(0, 0), (0, 3), (1, 0), (1, 2), (2, 0), (3, 2)\}$. Find S^t, the transitive closure of S.

53. Let $T = \{(0, 2), (1, 0), (2, 3), (3, 1)\}$. Find T^t, the transitive closure of T.

54. Write a computer algorithm to test whether a relation R defined on a finite set A is reflexive, where

$$A = \{a[1], a[2], \ldots, a[n]\}.$$

55. Write a computer algorithm to test whether a relation R defined on a finite set A is symmetric, where

$$A = \{a[1], a[2], \ldots, a[n]\}.$$

56. Write a computer algorithm to test whether a relation R defined on a finite set A is transitive, where

$$A = \{a[1], a[2], \ldots, a[n]\}.$$

ANSWERS FOR TEST YOURSELF

1. for every x in A, $x \, R \, x$ **2.** for every x and y in A, if $x \, R \, y$ then $y \, R \, x$ **3.** for every x, y, and z in A, if $x \, R \, y$ and $y \, R \, z$ then $x \, R \, z$ **4.** x is any element of A; $x \, R \, x$ **5.** x and y are any elements of A such that $x \, R \, y$; $y \, R \, x$ **6.** x, y, and z are any elements of A such that $x \, R \, y$ and $y \, R \, z$; $x \, R \, z$ **7.** show that there is an element x in A such that $x \not R \, x$ **8.** show that there are elements x and y in A such that $x \, R \, y$ but $y \not R \, x$ **9.** show that there are elements x, y, and z in A such that $x \, R \, y$ and $y \, R \, z$ but $x \not R \, z$ **10.** R^t is transitive; $R \subseteq R^t$; if S is any other transitive relation that contains R, then $R^t \subseteq S$

8.3 Equivalence Relations

"You are sad" the Knight said in an anxious tone: "let me sing you a song to comfort you."

. . . The name of the song is called 'Haddocks' Eyes.'"

"Oh, that's the name of the song, is it?" Alice said, trying to feel interested.

"No, you don't understand," the Knight said, looking a little vexed. "That's what the name is called. The name really is 'The Aged Aged Man.'"

"Then I ought to have said 'That's what the song is called'?" Alice corrected herself.

"No, you oughtn't: that's quite another thing! The song is called 'Ways and Means': but that's only what it's called, you know!"

"Well, what is the song, then?" said Alice, who was by this time completely bewildered.

"I was coming to that," the Knight said. "The song really is 'A-sitting on a Gate': and the tune's my own invention."

—Lewis Carroll, *Through the Looking Glass*, 1872

You know from your early study of fractions that each fraction has many equivalent forms. For example,

$$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{-1}{-2}, \frac{-3}{-6}, \frac{15}{30}, \ldots, \text{ and so on,}$$

are all different ways to represent the same number. They may look different; they may be called different names; but they are all equal. The idea of grouping together things that "look different but are really the same" is the central idea of equivalence relations.

The Relation Induced by a Partition

A **partition** of a set A is a finite or infinite collection of nonempty, mutually disjoint subsets whose union is A. The diagram of Figure 8.3.1 illustrates a partition of a set A by subsets $A_1, A_2, \ldots, A_6$.

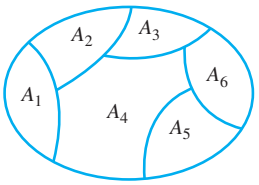


FIGURE 8.3.1 A Partition of a Set

Definition

Given a partition of a set A, the **relation induced by the partition**, R, is defined on A as follows: For every $x, y \in A$,

$$x \, R \, y \quad \Leftrightarrow \quad \text{there is a subset } A_i \text{ of the partition such that both } x \text{ and } y \text{ are in } A_i.$$

Example 8.3.1 **Relation Induced by a Partition**

Let $A = \{0, 1, 2, 3, 4\}$ and consider the following partition of A:

$$\{0, 3, 4\}, \{1\}, \{2\}.$$

Find the relation R induced by this partition.

Solution Since $\{0, 3, 4\}$ is a subset of the partition,

$0 \, R \, 3$ because both 0 and 3 are in $\{0, 3, 4\}$
$3 \, R \, 0$ because both 3 and 0 are in $\{0, 3, 4\}$
$0 \, R \, 4$ because both 0 and 4 are in $\{0, 3, 4\}$
$4 \, R \, 0$ because both 4 and 0 are in $\{0, 3, 4\}$
$3 \, R \, 4$ because both 3 and 4 are in $\{0, 3, 4\}$

Note These statements may seem strange, but, after all, they are not false!

and

$4 \, R \, 3$ because both 4 and 3 are in $\{0, 3, 4\}$.

Also,

$0 \, R \, 0$ because both 0 and 0 are in $\{0, 3, 4\}$
$3 \, R \, 3$ because both 3 and 3 are in $\{0, 3, 4\}$

and

$4 \, R \, 4$ because both 4 and 4 are in $\{0, 3, 4\}$.

Since $\{1\}$ is a subset of the partition,

$1 \, R \, 1$ because both 1 and 1 are in $\{1\}$,

and since $\{2\}$ is a subset of the partition,

$2 \, R \, 2$ because both 2 and 2 are in $\{2\}$.

Hence

$$R = \{(0, 0), (0, 3), (0, 4), (1, 1), (2, 2), (3, 0), (3, 3), (3, 4), (4, 0), (4, 3), (4, 4)\}.$$ ■

The fact is that a relation induced by a partition of a set satisfies all three properties studied in Section 8.2: reflexivity, symmetry, and transitivity.

Theorem 8.3.1

Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.

Proof: Suppose A is a set with a partition. In order to simplify notation, we assume that the partition consists of only a finite number of sets. The proof for an infinite partition is identical except for notation. Denote the partition subsets by

$$A_1, A_2, \ldots, A_n.$$

Then $A_i \cap A_j = \varnothing$ whenever $i \neq j$, and $A_1 \cup A_2 \cup \cdots \cup A_n = A$. The relation R induced by the partition is defined as follows: For every $x, y \in A$,

$$x \, R \, y \quad \Leftrightarrow \quad \text{there is a set } A_i \text{ of the partition such that } x \in A_i \text{ and } y \in A_i.$$

*[**Idea for the proof of reflexivity:** For R to be reflexive means that each element of A is related by R to itself. But by definition of R, for an element x to be related to itself means that x is in the same subset of the partition as itself. Well, if x is in some subset of the partition, then it is certainly in the same subset as itself. And x is in some subset of the partition because the union of the subsets of the partition is all of A. This reasoning is formalized as follows.]*

***Proof that R is reflexive*:** Suppose $x \in A$. Since $A_1, A_2, \ldots, A_n$ is a partition of A, it follows that $x \in A_i$ for some i, and so the statement

$$\text{there is a set } A_i \text{ of the partition such that } x \in A_i \text{ and } x \in A_i$$

is true. Thus, by definition of R, $x \, R \, x$.

Note The deduction that $x \in A_i$ and $x \in A_i$ is based on the logical equivalence of the statement forms p and $p \wedge p$.

*[**Idea for the proof of symmetry:** For R to be symmetric means that any time one element is related to a second, then the second is related to the first. Now for one element x to be related to a second element y means that x and y are in the same subset of the partition. But if this is the case, then y is in the same subset of the partition as x, so y is related to x by definition of R. This reasoning is formalized as follows.]*

***Proof that R is symmetric*:** Suppose x and y are elements of A such that $x \, R \, y$. Then

$$\text{there is a subset } A_i \text{ of the partition such that } x \in A_i \text{ and } y \in A_i$$

by definition of R. It follows that the statement

$$\text{there is a subset } A_i \text{ of the partition such that } y \in A_i \text{ and } x \in A_i$$

is also true. Hence, by definition of R, $y \, R \, x$.

Note The deduction that $y \in A_i$ and $x \in A_i$ is based on the logical equivalence of the statement forms $p \wedge q$ and $q \wedge p$.

(continued on page 508)

*[**Idea for the proof of transitivity:** For R to be transitive means that any time one element of A is related by R to a second and that second is related to a third, then the first element is related to the third. But for one element to be related to another means that there is a subset of the partition that contains both. So suppose x, y, and z are elements such that x is in the same subset as y and y is in the same subset as z. Must x be in the same subset as z? Yes, because the subsets of the partition are mutually disjoint. Since the subset that contains x and y has an element in common with the subset that contains y and z (namely, y), the two subsets are equal. But this means that x, y, and z are all in the same subset, and so, in particular, x and z are in the same subset. Hence x is related by R to z. This reasoning is formalized as follows.]*

***Proof that R is transitive*:** Suppose x, y, and z are in A and $x\ R\ y$ and $y\ R\ z$. By definition of R, there are subsets A_i and A_j of the partition such that

$$x \text{ and } y \text{ are in } A_i \quad \text{and} \quad y \text{ and } z \text{ are in } A_j.$$

Suppose $A_i \neq A_j$. *[We will deduce a contradiction.]* Then $A_i \cap A_j = \varnothing$ since $\{A_1, A_2, A_3, \ldots, A_n\}$ is a partition of A. But y is in A_i and y is in A_j also. Hence $A_i \cap A_j \neq \varnothing$. *[This contradicts the statement that $A_i \cap A_j = \varnothing$.]* Thus $A_i = A_j$. It follows that x, y, and z are all in A_i, and so, in particular,

$$x \text{ and } z \text{ are in } A_i.$$

Thus $x\ R\ z$ by definition of R.

Definition of an Equivalence Relation

A relation on a set that satisfies the three properties of reflexivity, symmetry, and transitivity is called an *equivalence relation*.

Definition

Let A be a set and R a relation on A. R is an **equivalence relation** if, and only if, R is reflexive, symmetric, and transitive.

Thus, according to Theorem 8.3.1, the relation induced by a partition is an equivalence relation. A variety of additional examples of equivalence relations are given below and in the exercises.

Example 8.3.2 **An Equivalence Relation on a Set of Subsets**

Let X be the set of all nonempty subsets of {1, 2, 3}. Then

$$X = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Define a relation $\mathbf{R}$ on X as follows: For every A and B in X,

$$A\ \mathbf{R}\ B \Leftrightarrow \text{the least element of } A \text{ equals the least element of } B.$$

Prove that $\mathbf{R}$ is an equivalence relation on X.

Solution

$\mathbf{R}$ *is reflexive*: Suppose A is a nonempty subset of {1, 2, 3}. *[We must show that $A\ \mathbf{R}\ A$.]* It is true to say that the least element of A equals the least element of A. Thus, by definition of $\mathbf{R}$, $A\ \mathbf{R}\ A$.

R *is symmetric*: Suppose A and B are nonempty subsets of $\{1, 2, 3\}$ and $A \mathbf{R} B$. *[We must show that* $B \mathbf{R} A$*.]* Since $A \mathbf{R} B$, the least element of A equals the least element of B. But this implies that the least element of B equals the least element of A, and so, by definition of $\mathbf{R}$, $B \mathbf{R} A$.

R *is transitive*: Suppose A, B, and C are nonempty subsets of $\{1, 2, 3\}$, $A \mathbf{R} B$, and $B \mathbf{R} C$. *[We must show that* $A \mathbf{R} C$*.]* Since $A \mathbf{R} B$, the least element of A equals the least element of B and since $B \mathbf{R} C$, the least element of B equals the least element of C. Thus the least element of A equals the least element of C, and so, by definition of $\mathbf{R}$, $A \mathbf{R} C$. ■

Example 8.3.3 **Equivalence of Digital Logic Circuits Is an Equivalence Relation**

Let S be the set of all digital logic circuits with a fixed number n of inputs. Define a relation $\mathbf{E}$ on S as follows: For all circuits C_1 and C_2 in S,

$$C_1 \mathbf{E} C_2 \quad \Leftrightarrow \quad C_1 \text{ has the same input/output table as } C_2.$$

If $C_1 \mathbf{E} C_2$, then circuit C_1 is said to be *equivalent* to circuit C_2. Prove that $\mathbf{E}$ is an equivalence relation on S.

Solution

E *is reflexive*: Suppose C is a digital logic circuit in S. *[We must show that* $C \mathbf{E} C$*.]* Certainly C has the same input/output table as itself. Thus, by definition of $\mathbf{E}$, $C \mathbf{E} C$ *[as was to be shown].*

E *is symmetric*: Suppose C_1 and C_2 are digital logic circuits in S such that $C_1 \mathbf{E} C_2$. *[We must show that* $C_2 \mathbf{E} C_1$*.]* By definition of $\mathbf{E}$, since $C_1 \mathbf{E} C_2$, then C_1 has the same input/output table as C_2. It follows that C_2 has the same input/output table as C_1. Hence, by definition of $\mathbf{E}$, $C_2 \mathbf{E} C_1$ *[as was to be shown].*

E *is transitive*: Suppose C_1, C_2, and C_3 are digital logic circuits in S such that $C_1 \mathbf{E} C_2$ and $C_2 \mathbf{E} C_3$. *[We must show that* $C_1 \mathbf{E} C_3$*.]* By definition of $\mathbf{E}$, since $C_1 \mathbf{E} C_2$ and $C_2 \mathbf{E} C_3$, then

$$C_1 \text{ has the same input/output table as } C_2$$

and

$$C_2 \text{ has the same input/output table as } C_3.$$

It follows that

$$C_1 \text{ has the same input/output table as } C_3.$$

Hence, by definition of $\mathbf{E}$, $C_1 \mathbf{E} C_3$ *[as was to be shown].*

Since $\mathbf{E}$ is reflexive, symmetric, and transitive, $\mathbf{E}$ is an equivalence relation on S. ■

Certain implementations of computer languages do not place a limit on the allowable length of an identifier. This permits a programmer to be as precise as necessary in naming variables without having to worry about exceeding length limitations. However, compilers for such languages often ignore all but some specified number of initial characters: As far as the compiler is concerned, two identifiers are the same if they have the same initial characters, even though they may look different to a human reader of the program. For example, to a compiler that ignores all but the first eight characters of an identifier, the following identifiers would be the same:

NumberOfScrews NumberOfBolts.

Obviously, in using such a language, the programmer has to be sure to avoid giving two distinct identifiers the same first eight characters. When a compiler lumps identifiers together in this way, it sets up an equivalence relation on the set of all possible identifiers in the language. Such a relation is described in the next example.

Example 8.3.4 **A Relation on a Set of Identifiers**

Let L be the set of all allowable identifiers in a certain computer language, and define a relation R on L as follows: For all strings s and t in L,

$$s \, R \, t \quad \Leftrightarrow \quad \text{the first eight characters of } s \text{ equal the first eight characters of } t.$$

Prove that R is an equivalence relation on L.

Solution

***R is reflexive*:** Let $s \in L$. *[We must show that $s \, R \, s$.]* Clearly s has the same first eight characters as itself. Thus, by definition of R, $s \, R \, s$ *[as was to be shown].*

***R is symmetric*:** Let s and t be in L and suppose that $s \, R \, t$. *[We must show that $t \, R \, s$.]* By definition of R, since $s \, R \, t$, the first eight characters of s equal the first eight characters of t. It follows that the first eight characters of t equal the first eight characters of s, and so, by definition of R, $t \, R \, s$ *[as was to be shown].*

***R is transitive*:** Let s, t, and u be in L and suppose that $s \, R \, t$ and $t \, R \, u$. *[We must show that $s \, R \, u$.]* By definition of R, since $s \, R \, t$ and $t \, R \, u$, the first eight characters of s equal the first eight characters of t, and the first eight characters of t equal the first eight characters of u. Hence the first eight characters of s equal the first eight characters of u. Hence, by definition of R, $s \, R \, u$ *[as was to be shown].*

Since R is reflexive, symmetric, and transitive, R is an equivalence relation on L. ■

Equivalence Classes of an Equivalence Relation

Suppose there is an equivalence relation on a certain set. If a is any particular element of the set, then one can ask, "What is the subset of all elements that are related to a?" This subset is called the *equivalence class* of a.

Note Be careful to distinguish among the following: (1) a relation on a set, (2) the (underlying) set itself, and (3) the equivalence class for an element of the (underlying) set.

Definition

Suppose A is a set and R is an equivalence relation on A. For each element a in A, the **equivalence class of a**, denoted **$[a]$** and called the **class of a** for short, is the set of all elements x in A such that x is related to a by R.

In symbols:

$$[a] = \{x \in A \mid x \, R \, a\}$$

The procedural version of this definition is

$$\text{for every } x \in A, \quad x \in [a] \quad \Leftrightarrow \quad x \, R \, a.$$

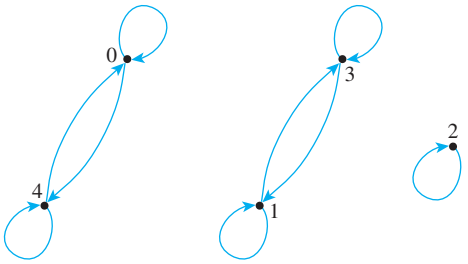
When several equivalence relations on a set are under discussion, the notation $[a]_R$ may be used to denote the equivalence class of a for the relation R.

Example 8.3.5 **Equivalence Classes of a Relation Given as a Set of Ordered Pairs**

Let $A = \{0, 1, 2, 3, 4\}$ and define a relation R on A as follows:

$$R = \{(0, 0), (0, 4), (1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 0), (4, 4)\}.$$

The directed graph for R is as shown below. As can be seen by inspection, R is an equivalence relation on A. Find the distinct equivalence classes of R.



Solution First find the equivalence class of every element of A.

$$[0] = \{x \in A \mid x\,R\,0\} = \{0, 4\}$$
$$[1] = \{x \in A \mid x\,R\,1\} = \{1, 3\}$$
$$[2] = \{x \in A \mid x\,R\,2\} = \{2\}$$
$$[3] = \{x \in A \mid x\,R\,3\} = \{1, 3\}$$
$$[4] = \{x \in A \mid x\,R\,4\} = \{0, 4\}$$

Note that $[0] = [4]$ and $[1] = [3]$. Thus the *distinct* equivalence classes of the relation are

$$\{0, 4\},\ \{1, 3\},\ \text{and}\ \{2\}.$$ ■

When a problem asks you to find the *distinct* equivalence classes of an equivalence relation, you will generally solve the problem in two steps. In the first step you either explicitly construct (as in Example 8.3.5) or imagine constructing (as in infinite cases) the equivalence class for each element of the domain A of the relation. Usually several of the classes will contain exactly the same elements, so in the second step you must take a careful look at the classes to determine which are the same. You then indicate the distinct equivalence classes by describing them without duplication.

Example 8.3.6 **Equivalence Classes of a Relation on a Set of Subsets**

In Example 8.3.2 it was shown that the relation **R** was an equivalence relation, where for nonempty subsets A and B of $\{1, 2, 3\}$ to be related by **R** means that they have the same least element. Describe the distinct equivalence classes of **R**.

Solution The equivalence class of $\{1\}$ is the set of all the nonempty subsets of $\{1, 2, 3\}$ whose least element is 1. Thus

$$[\{1\}] = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}.$$

The equivalence class of $\{2\}$ is the set of all the nonempty subsets of $\{1, 2, 3\}$ whose least element is 2. Thus

$$[\{2\}] = \{\{2\}, \{2, 3\}\}.$$

The equivalence class of {3} is the set of all the nonempty subsets of {1, 2, 3} whose least element is 3. There is only one such set: {3} itself. Thus

$$[\{3\}] = \{\{3\}\}.$$

Since all the nonempty subsets of {1, 2, 3} are in one of the equivalence classes, this is a complete listing. Moreover, these classes are all distinct. ■

Example 8.3.7 **Equivalence Classes of Identifiers**

In Example 8.3.4 it was shown that the relation R of having the same first eight characters is an equivalence relation on the set L of allowable identifiers in a computer language. Describe the distinct equivalence classes of R.

Solution By definition of R, two strings in L are related by R if, and only if, they have the same first eight characters. Given any string s in L,

$$\begin{aligned}[s] &= \{t \in L \mid t\, R\, s\} \\ &= \{t \in L \mid \text{the first eight characters of } t \text{ equal the first eight characters of } s\}.\end{aligned}$$

Thus the distinct equivalence classes of R are sets of strings such that (1) each class consists entirely of strings all of which have the same first eight characters, and (2) any two distinct classes contain strings that differ somewhere in their first eight characters. ■

Example 8.3.8 **Equivalence Classes of the Identity Relation**

Let A be any set and define a relation R on A as follows: For every x and y in A,

$$x\, R\, y \quad \Leftrightarrow \quad x = y.$$

Then R is an equivalence relation. *[To prove this, just generalize the argument used in Example 8.2.2.]* Describe the distinct equivalence classes of R.

Solution Given any a in A, the class of a is

$$[a] = \{x \in A \mid x\, R\, a\}.$$

Now by definition of R, $a\, R\, x$ if, and only if, $a = x$. So

$$\begin{aligned}[a] &= \{x \in A \mid x = a\} \\ &= \{a\} \qquad \text{since the only element of } A \text{ that equals } a \text{ is } a.\end{aligned}$$

Hence, given any a in A,

$$[a] = \{a\},$$

and if $x \neq a$ then $\{x\} \neq \{a\}$. Consequently, all the classes of all the elements of A are distinct, and the distinct equivalence classes of R are all the single-element subsets of A. ■

In each of Examples 8.3.5, 8.3.6, 8.3.7, and 8.3.8, the set of distinct equivalence classes of the relation consists of mutually disjoint subsets whose union is the entire domain A of the relation. This means that the set of equivalence classes of the relation forms a partition of the domain A. In fact, it is always the case that the equivalence classes of an equivalence relation partition the domain of the relation into a union of mutually disjoint subsets. We establish the truth of this statement in stages, first proving two lemmas and then proving the main theorem.

The first lemma says that if two elements of A are related by an equivalence relation R, then their equivalence classes are the same.

Lemma 8.3.2

Suppose A is a set, R is an equivalence relation on A, and a and b are elements of A. If $a \, R \, b$, then $[a] = [b]$.

This lemma says that if a certain condition is satisfied, then $[a] = [b]$. Now $[a]$ and $[b]$ are *sets*, and two sets are equal if, and only if, each is a subset of the other. Hence the proof of the lemma consists of two parts: first, a proof that $[a] \subseteq [b]$ and second, a proof that $[b] \subseteq [a]$. To show each subset relation, it is necessary to show that every element in the left-hand set is an element of the right-hand set.

Proof of Lemma 8.3.2:

Let A be a set, let R be an equivalence relation on A, and suppose

a and b are elements of A such that $a \, R \, b$.

[We must show that $[a] = [b]$*.]*

Proof that $[a] \subseteq [b]$**:** Let $x \in [a]$. *[We must show that* $x \in [b]$*.]* Since

$$x \in [a],$$

then

$$x \, R \, a$$

by definition of class. But

$$a \, R \, b$$

by hypothesis. Thus, by transitivity of R,

$$x \, R \, b.$$

Hence

$$x \in [b]$$

by definition of class. *[This is what was to be shown.]*

Proof that $[b] \subseteq [a]$**:** Let $x \in [b]$. *[We must show that* $x \in [a]$*.]* Since

$$x \in [b]$$

then

$$x \, R \, b$$

by definition of class. Now

$$a \, R \, b$$

by hypothesis. Thus, since R is symmetric,

$$b \, R \, a$$

also. Then, since R is transitive and $x \, R \, b$ and $b \, R \, a$,

$$x \, R \, a.$$

Hence,

$$x \in [a]$$

by definition of class. *[This is what was to be shown.]*

Since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, it follows that $[a] = [b]$ by definition of set equality.

The second lemma says that any two equivalence classes of an equivalence relation are either mutually disjoint or identical.

Lemma 8.3.3

If A is a set, R is an equivalence relation on A, and a and b are elements of A, then

$$\text{either} \quad [a] \cap [b] = \varnothing \quad \text{or} \quad [a] = [b].$$

The statement of Lemma 8.3.3 has the form

$$\text{if } p \text{ then } (q \text{ or } r),$$

Note You can always prove a statement of the form "if p then (q or r)" by proving one of the logically equivalent statements: "if (p and not q) then r" or "if (p and not r) then q."*

where p is the statement "A is a set, R is an equivalence relation on A, and a and b are elements of A," q is the statement "$[a] \cap [b] = \varnothing$," and r is the statement "$[a] = [b]$." To prove the lemma, we will prove the logically equivalent statement

$$\text{if } (p \text{ and not } q) \text{ then } r.$$

That is, we will prove the following:

> If A is a set, R is an equivalence relation on A, a and b are elements of A, and $[a] \cap [b] \neq \varnothing$, then $[a] = [b]$.

Proof of Lemma 8.3.3:

Suppose A is a set, R is an equivalence relation on A, a and b are elements of A, and

$$[a] \cap [b] \neq \varnothing.$$

[We must show that $[a] = [b]$*.]* Since $[a] \cap [b] \neq \varnothing$, there exists an element x in A such that $x \in [a] \cap [b]$. By definition of intersection,

$$x \in [a] \quad \text{and} \quad x \in [b],$$

and so

$$x \, R \, a \quad \text{and} \quad x \, R \, b$$

by definition of class. Since R is symmetric *[being an equivalence relation]* and $x \, R \, a$, then $a \, R \, x$. But R is also transitive *[since it is an equivalence relation],* and so, since $a \, R \, x$ and $x \, R \, b$,

$$a \, R \, b.$$

Now a and b satisfy the hypothesis of Lemma 8.3.2. Hence, by that lemma,

$$[a] = [b]$$

[as was to be shown].

Theorem 8.3.4 The Partition Induced by an Equivalence Relation

If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any two distinct classes is empty.

*See exercise 14 in Section 2.2.

The proof of Theorem 8.3.4 is divided into two parts: first, a proof that A is the union of the equivalence classes of R and second, a proof that the intersection of any two distinct equivalence classes is empty. The proof of the first part follows from the fact that the relation is reflexive. The proof of the second part follows from Lemma 8.3.3.

Proof of Theorem 8.3.4:

Suppose A is a set and R is an equivalence relation on A. For notational simplicity, we assume that R has only a finite number of distinct equivalence classes, which we denote

$$A_1, A_2, \ldots, A_n,$$

where n is a positive integer. (When the number of classes is infinite, the proof is identical except for notation.)

Proof that $A = A_1 \cup A_2 \cup \cdots \cup A_n$: *[We must show that $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$ and that $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$.]*

To show that $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$, suppose x is any element of A. *[We must show that $x \in A_1 \cup A_2 \cup \cdots \cup A_n$.]* By reflexivity of R, $x\ R\ x$. And this implies that $x \in [x]$ by definition of class. Since x is in *some* equivalence class, it must be in one of the distinct equivalence classes $A_1, A_2, \ldots,$ or A_n. Thus $x \in A_i$ for some index i, and hence $x \in A_1 \cup A_2 \cup \cdots \cup A_n$ by definition of union *[as was to be shown].*

To show that $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$, suppose $x \in A_1 \cup A_2 \cup \cdots \cup A_n$. *[We must show that $x \in A$.]* Then $x \in A_i$ for some $i = 1, 2, \ldots, n$, by definition of union. Now each A_i is an equivalence class of R, and equivalence classes are subsets of A. Hence $A_i \subseteq A$ and so $x \in A$ *[as was to be shown].*

Since $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$ and $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$, then by definition of set equality, $A = A_1 \cup A_2 \cup \cdots \cup A_n$.

***Proof that the distinct classes of R are mutually disjoint*:** Suppose that A_i and A_j are any two distinct equivalence classes of R. *[We must show that A_i and A_j are disjoint.]* Since A_i and A_j are distinct, then $A_i \neq A_j$. And since A_i and A_j are equivalence classes of R, there must exist elements a and b in A such that $A_i = [a]$ and $A_j = [b]$. By Lemma 8.3.3,

$$\text{either } [a] \cap [b] = \varnothing \quad \text{or} \quad [a] = [b].$$

Now $[a] \neq [b]$ because $A_i \neq A_j$, and hence $[a] \cap [b] = \varnothing$. Thus $A_i \cap A_j = \varnothing$, and so A_i and A_j are disjoint *[as was to be shown].*

Example 8.3.9 **Equivalence Classes of Digital Logic Circuits**

In Example 8.3.3 it was shown that the relation of equivalence among circuits is an equivalence relation. Let S be the set of all digital logic circuits with exactly two inputs and one output. The binary relation $\mathbf{E}$ is defined on S as follows: For every C_1 and C_2 in S,

$$C_1\ \mathbf{E}\ C_2 \quad \Leftrightarrow \quad C_1 \text{ has the same input/output table as } C_2.$$

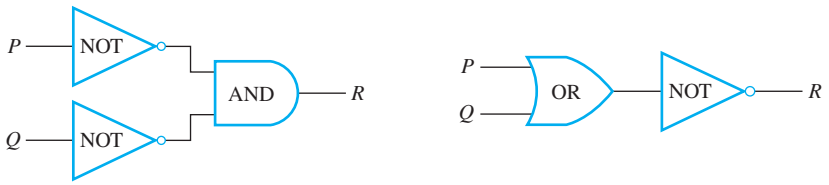
Describe the equivalence classes of this relation. How many distinct equivalence classes are there? Find two different circuits that are in one of the classes.

Solution Given a circuit C, the equivalence class of C is the set of all circuits with two input signals and one output signal that have the same input/output table as C. Now each input/output table has exactly four rows, corresponding to the four possible combinations of inputs: 11, 10, 01, and 00. A typical input/output table is the following:

Input		Output
P	Q	R
1	1	0
1	0	0
0	1	0
0	0	1

There are exactly as many such tables as there are binary strings of length 4. The reason is that distinct input/output tables can be formed by changing the pattern of the four 0's and 1's in the output column, and there are as many ways to do that as there are strings of four 0's and 1's. And since the number of binary strings of length 4 is $2^4 = 16$, there are 16 distinct input/output tables.

This implies that there are exactly 16 equivalence classes of circuits, one for each distinct input/output table. However, there are infinitely many circuits that give rise to each table. For instance, two circuits for the previous input/output table are shown below.



■

Congruence Modulo n

Example 8.2.4 showed that the relation of congruence modulo 3 is reflexive, symmetric, and transitive. Therefore, it is an equivalence relation.

Example 8.3.10 **Equivalence Classes of Congruence Modulo 3**

Let R be the relation of congruence modulo 3 on the set $\mathbf{Z}$ of all integers. That is, for all integers m and n,

$$m \, R \, n \quad \Leftrightarrow \quad 3 \mid (m - n).$$

Describe the distinct equivalence classes of R.

Solution For each integer a,

$$\begin{aligned} [a] &= \{x \in \mathbf{Z} \mid x \, R \, a\} \\ &= \{x \in \mathbf{Z} \mid 3 \mid (x - a)\} \\ &= \{x \in \mathbf{Z} \mid x - a = 3k, \text{ for some integer } k\}. \end{aligned}$$

Therefore,

$$[a] = \{x \in Z \mid x = 3k + a, \text{ for some integer } k\}.$$

In particular,

$$\begin{aligned}[0] &= \{x \in \mathbf{Z} \mid x = 3k + 0, \text{ for some integer } k\} \\ &= \{x \in \mathbf{Z} \mid x = 3k, \text{ for some integer } k\} \\ &= \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}, \\ [1] &= \{x \in \mathbf{Z} \mid x = 3k + 1, \text{ for some integer } k\} \\ &= \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}, \\ [2] &= \{x \in \mathbf{Z} \mid x = 3k + 2, \text{ for some integer } k\} \\ &= \{\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\}.\end{aligned}$$

Now since $3 \; R \; 0$, then by Lemma 8.3.2,

$$[3] = [0].$$

More generally, by the same reasoning,

$$[0] = [3] = [-3] = [6] = [-6] = \ldots, \text{ and so on.}$$

Similarly,

$$[1] = [4] = [-2] = [7] = [-5] = \ldots, \text{ and so on.}$$

And

$$[2] = [5] = [-1] = [8] = [-4] = \ldots, \text{ and so on.}$$

Notice that every integer is in class [0], [1], or [2]. Hence the distinct equivalence classes are

$$\{x \in \mathbf{Z} \mid x = 3k, \text{ for some integer } k\},$$

$$\{x \in \mathbf{Z} \mid x = 3k + 1, \text{ for some integer } k\}, \quad \text{and}$$

$$\{x \in \mathbf{Z} \mid x = 3k + 2, \text{ for some integer } k\}.$$

In words, the three classes of congruence modulo 3 are (1) the set of all integers that are divisible by 3, (2) the set of all integers that leave a remainder of 1 when divided by 3, and (3) the set of all integers that leave a remainder of 2 when divided by 3. ■

Example 8.3.10 illustrates a very important property of equivalence classes, namely that an equivalence class may have many different names. In Example 8.3.10, for instance, the class of 0, [0], may also be *called* the class of 3, [3], or the class of -6, $[-6]$. But what the class *is* is the set of all integers that are divisible by 3:

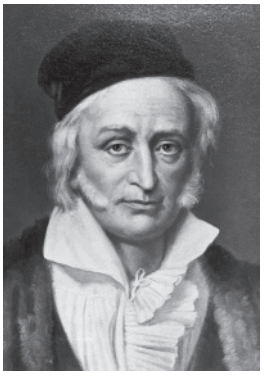
$$\{x \in \mathbf{Z} \mid x = 3k, \text{ for some integers } k\}.$$

(The quote at the beginning of this section refers in a humorous way to the philosophically interesting distinction between what things are *called* and what they *are*.)

Definition

Suppose R is an equivalence relation on a set A and S is an equivalence class of R. A **representative** of the class S is any element a such that $[a] = S$.

In exercises 36–41 at the end of this section, you are asked to show, in effect, that if a is any element of an equivalence class S, then $S = [a]$. Hence *any* element of an equivalence class is a representative of that class.



Bettmann/Getty Images

Carl Friedrich Gauss (1777–1855)

The following notation is used frequently when referring to congruence relations. It was introduced by Carl Friedrich Gauss in the first chapter of his book *Disquisitiones Arithmeticae*. This work, which was published when Gauss was only 24, laid the foundation for modern number theory.

Definition

Let m and n be integers and let d be a positive integer. We say that ***m* is congruent to *n* modulo *d*** and write

$$m \equiv n \pmod{d}$$

if, and only if, $d \mid (m - n)$.

Symbolically: $m \equiv n \pmod{d} \iff d \mid (m - n)$.

Exercise 17(b) at the end of this section asks you to show that $m \equiv n \pmod{d}$ if, and only if, $m \bmod d = n \bmod d$, where m, n, and d are integers and d is positive.

Example 8.3.11 **Evaluating Congruences**

Determine which of the following congruences are true and which are false.

a. $12 \equiv 7 \pmod{5}$ b. $6 \equiv -8 \pmod{4}$ c. $3 \equiv 3 \pmod{7}$

Solution

a. True. $12 - 7 = 5 = 5 \cdot 1$. Hence $5 \mid (12 - 7)$, and so $12 \equiv 7 \pmod{5}$.

b. False. $6 - (-8) = 14$, and $4 \nmid 14$ because $14 \neq 4 \cdot k$ for any integer k. Consequently, $6 \not\equiv -8 \pmod{4}$.

c. True. $3 - 3 = 0 = 7 \cdot 0$. Hence $7 \mid (3 - 3)$, and so $3 \equiv 3 \pmod{7}$. ■

The discussion of binary arithmetic in Section 2.5 used a simplified computer model, which used 8-bit two's complements and binary arithmetic to represent and compute with the 256 integers from -128 to $127 - 1$. To find $78 + (-46)$, the following scheme was shown:

	0	1	0	0	1	1	1	0	↔ 78
+	1	1	0	1	0	0	1	0	↔ −46
1	0	0	1	0	0	0	0	0	

Now the number corresponding to 100100000_2 is 288, which is too large to be the 8-bit binary representation of a number. But the directions said to discard the 1 in the 2^9th position. When this is done, the result is 00100000_2, which corresponds to 32 and is the correct answer for the problem.

To see why this method works, observe that the decimal forms of the two's complements for 78 and -46 are 78 and $2^8 - 46$, respectively. In addition,

$$78 + (2^8 - 46) = 2^8 + (78 - 46) \equiv (78 - 46) \pmod{2^8}.$$

Thus reducing the number $78 + (2^8 - 46)$ modulo 2^8 gives the correct result. And doing so is equivalent to dropping the 1 in the 2^9th position of the computation's result because the 2^9th position holds the place for the number 2^8 when integers are represented in binary notation.

A Definition for Rational Numbers

For a moment, forget what you know about fractional arithmetic and look at the numbers

$$\frac{1}{3} \quad \text{and} \quad \frac{2}{6}$$

as *symbols*. Considered as symbolic expressions, these *appear* quite different. In fact, if they were written as ordered pairs

$$(1, 3) \quad \text{and} \quad (2, 6)$$

they would *be* different. The fact that we regard them as "the same" is a specific instance of our general agreement to regard any two numbers

$$\frac{a}{b} \quad \text{and} \quad \frac{c}{d}$$

as equal provided the *cross products* are equal; in other words, if, and only if, $ad = bc$. This can be formalized as follows, using the language of equivalence relations.

Example 8.3.12 **Rational Numbers Are Really Equivalence Classes**

Let A be the set of all ordered pairs of integers for which the second element of the pair is nonzero. Symbolically:

$$A = \mathbf{Z} \times (\mathbf{Z} - \{0\}).$$

Define a relation R on A as follows: For all pairs (a, b) and (c, d) in A,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad ad = bc.$$

The fact is that R is an equivalence relation.

a. Prove that R is transitive. (Proofs that R is reflexive and symmetric are left to exercise 42 at the end of the section.)

b. Describe the distinct equivalence classes of R.

Solution

a. *[We must show that for all ordered pairs* (a, b), (c, d), and (e, f) in A, *if* $(a, b)\ R\ (c, d)$ *and* $(c, d)\ R\ (e, f)$, *then* $(a, b)\ R\ (e, f)$.*]* Suppose (a, b), (c, d), and (e, f) are particular but arbitrarily chosen elements of A such that $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (e, f)$. *[We must show that* $(a, b)\ R\ (e, f)$.*]* By definition of R,

$$(1)\ ad = bc \quad \text{and} \quad (2)\ cf = de.$$

Since the second elements of all ordered pairs in A are nonzero, $b \neq 0$, $d \neq 0$, and $f \neq 0$. Multiply both sides of equation (1) by f and both sides of equation (2) by b to obtain

$$(1')\ adf = bcf \quad \text{and} \quad (2')\ bcf = bde.$$

Because both equal bcf,

$$adf = bde,$$

and, since $d \neq 0$, it follows from the cancellation law for multiplication (T7 in Appendix A) that

$$af = be.$$

Hence, by definition of R, $(a, b)\ R\ (e, f)$ *[as was to be shown].*

b. There is one equivalence class for each distinct rational number. Each equivalence class consists of all ordered pairs (a, b) that, if written as fractions a/b, would equal each other. The reason is that the condition for two rational numbers to be equal is the same as the condition for two ordered pairs to be related. For instance, the class of (1, 2) is

$$[(1, 2)] = \{(1, 2), (-1, -2), (2, 4), (-2, -4), (3, 6), (-3, -6), \dots\}$$

since $\frac{1}{2} = \frac{-1}{-2} = \frac{2}{4} = \frac{-2}{-4} = \frac{3}{6} = \frac{-3}{-6}$ and so forth. ■

It is possible to expand the result of Example 8.3.12 to define operations of addition and multiplication on the equivalence classes of R that satisfy all the same properties as the addition and multiplication of rational numbers. (See exercise 43.) It follows that the rational numbers can be defined as equivalence classes of ordered pairs of integers. Similarly (see exercise 44), it can be shown that all integers, negative and zero included, can be defined as equivalence classes of ordered pairs of positive integers. In the late nineteenth century, F. L. G. Frege and Giuseppe Peano showed that the positive integers can be defined entirely in terms of sets. And just a little earlier, Richard Dedekind (1848–1916) showed that all real numbers can be defined as sets of rational numbers. Taken together, these results show that the set of real numbers can be defined using logic and set theory alone.

TEST YOURSELF

1. For a relation on a set to be an equivalence relation, it must be _____.
2. The notation $m \equiv n \pmod{d}$ is read "_____" and means that _____.
3. Given an equivalence relation R on a set A and given an element a in A, the equivalence class of a is denoted _____ and is defined to be _____.
4. If A is a set, R is an equivalence relation on A, and a and b are elements of A, then either $[a] = [b]$ or _____.
5. If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form _____.
6. Let $A = \mathbf{Z} \times (\mathbf{Z} - \{0\})$, and define a relation R on A by specifying that for every (a, b) and (c, d) in A, $(a, b)\ R\ (c, d)$ if, and only if, $ad = bc$. Then there is exactly one equivalence class of R for each _____.

EXERCISE SET 8.3

1. Suppose that $S = \{a, b, c, d, e\}$ and R is a relation on S such that $a\ R\ b$, $b\ R\ c$, and $d\ R\ e$. List all of the following that must be true if R is (a) reflexive (but not symmetric or transitive), (b) symmetric (but not reflexive or transitive), (c) transitive (but not reflexive or symmetric), and (d) an equivalence relation.
   $c\ R\ b$ $\quad c\ R\ c$ $\quad a\ R\ c$ $\quad b\ R\ a$
   $a\ R\ d$ $\quad e\ R\ a$ $\quad e\ R\ d$ $\quad c\ R\ a$
2. Each of the following partitions of $\{0, 1, 2, 3, 4\}$ induces a relation R on $\{0, 1, 2, 3, 4\}$. In each case, find the ordered pairs in R.
   a. $\{0, 2\}, \{1\}, \{3, 4\}$ **b.** $\{0\}, \{1, 3, 4\}, \{2\}$
   c. $\{0\}, \{1, 2, 3, 4\}$

In each of 3–6, the relation R is an equivalence relation on A. As in Example 8.3.5, first find the specified equivalence classes. Then state the number of distinct equivalence classes for R and list them.

3. $A = \{0, 1, 2, 3, 4\}$
   $R = \{(0, 0), (0, 4), (1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 0), (4, 4)\}$
   equivalence classes: [0], [1], [2], [3]
4. $A = \{a, b, c, d\}$
   $R = \{(a, a), (b, b), (b, d), (c, c), (d, b), (d, d)\}$
   equivalence classes: $[a]$, $[b]$, $[c]$, $[d]$

5. $A = \{1, 2, 3, 4, \ldots, 20\}$. R is defined on A as follows:

$$\text{For all } x, y \in A, \quad x \, R \, y \iff 4 \mid (x - y).$$

equivalence classes: [1], [2], [3], [4], [5]

6. $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R is defined on A as follows:

$$\text{For all } x, y \in A, \quad x \, R \, y \iff 3 \mid (x - y).$$

equivalence classes: [0], [1], [2], [3]

In each of 7–14, the relation R is an equivalence relation on the set A. Find the distinct equivalence classes of R.

7. $A = \{(1, 3), (2, 4), (-4, -8), (3, 9), (1, 5), (3, 6)\}$. R is defined on A as follows: For every (a, b), $(c, d) \in A$,

$$(a, b) \, R \, (c, d) \iff ad = bc.$$

8. $X = \{a, b, c\}$ and $A = \mathcal{P}(X)$. R is defined on A as follows: For all sets U and V in $\mathcal{P}(X)$,

$$U \, R \, V \iff N(U) = N(V).$$

(That is, the number of elements in U equals the number of elements in V.)

9. $X = \{-1, 0, 1\}$ and $A = \mathcal{P}(X)$. R is defined on $\mathcal{P}(X)$ as follows: For all sets S and T in $\mathcal{P}(X)$,

$$S \, R \, T \iff \text{the sum of the elements in } S \text{ equals the sum of the elements in } T.$$

10. $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R is defined on A as follows: For all $m, n \in \mathbf{Z}$,

$$m \, R \, n \iff 3 \mid (m^2 - n^2).$$

11. $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. R is defined on A as follows: For every $(m, n) \in A$,

$$m \, R \, n \iff 4 \mid (m^2 - n^2).$$

12. $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. R is defined on A as follows: For all $(m, n) \in A$,

$$m \, R \, n \iff 5 \mid (m^2 - n^2).$$

13. A is the set of all strings of length 4 in a's and b's. R is defined on A as follows: For all strings s and t in A,

$s \, R \, t \iff s$ has the same first two characters as t.

14. A is the set of all strings of 0's, 1's, and 2's that have length 4 and for which the sum of the characters in the string is less than or equal to 2. R is defined on A as follows: For every $s, t \in A$,

$s \, R \, t \iff$ the sum of the characters of s equals the sum of the characters of t.

15. Determine which of the following congruence relations are true and which are false.

a. $17 \equiv 2 \pmod 5$

b. $4 \equiv -5 \pmod 7$

c. $-2 \equiv -8 \pmod 3$

d. $-6 \equiv 22 \pmod 2$

16. a. Let R be the relation of congruence modulo 3. Which of the following equivalence classes are equal?

$$[7], [-4], [-6], [17], [4], [27], [19]$$

b. Let R be the relation of congruence modulo 7. Which of the following equivalence classes are equal?

$$[35], [3], [-7], [12], [0], [-2], [17]$$

17. a. Prove that for all integers m and n, $m \equiv n \pmod 3$ if, and only if, $m \bmod 3 = n \bmod 3$.

b. Prove that for all integers m and n and any positive integer d, $m \equiv n \pmod d$ if, and only if, $m \bmod d = n \bmod d$.

18. a. Give an example of two sets that are distinct but not disjoint.

b. Find sets A_1 and A_2 and elements x, y, and z such that x and y are in A_1 and y and z are in A_2 but x and z are not both in either of the sets A_1 or A_2.

In 19–31, (1) prove that the relation is an equivalence relation, and (2) describe the distinct equivalence classes of each relation.

19. A is the set of all students at your college.

a. R is the relation defined on A as follows: For every x and y in A,

$$x \, R \, y \iff x \text{ has the same major (or double major) as } y.$$

(Assume "undeclared" is a major.)

b. S is the relation defined on A as follows: For every $x, y \in A$,

$$x \, S \, y \iff x \text{ is the same age as } y.$$

20. E is the relation defined on $\mathbf{Z}$ as follows:

$$\text{For every } m, n \in \mathbf{Z}, \quad m \, E \, n \iff 4 \mid (m - n).$$

***H* 21.** R is the relation defined on $\mathbf{Z}$ as follows:

$$\text{For every } m, n \in \mathbf{Z}, \quad m \, R \, n \iff 7m - 5n \text{ is even.}$$

22. Let A be the set of all statement forms in three variables p, q, and r. $\mathbf{R}$ is the relation defined on A as follows: For all P and Q in A,

$$P \mathbf{R} Q \iff P \text{ and } Q \text{ have the same truth table.}$$

23. Let P be a set of parts shipped to a company from various suppliers. S is the relation defined on P as follows: For every $x, y \in P$,

$$x S y \iff x \text{ has the same part number and is shipped from the same supplier as } y.$$

24. Let A be the set of identifiers in a computer program. It is common for identifiers to be used for only a short part of the execution time of a program and not to be used again to execute other parts of the program. In such cases, arranging for identifiers to share memory locations makes efficient use of a computer's memory capacity. Define a relation R on A as follows: For all identifiers x and y,

$$x R y \iff \text{the values of } x \text{ and } y \text{ are stored in the same memory location during execution of the program.}$$

25. A is the "absolute value" relation defined on $\mathbf{R}$ as follows:

$$\text{For every } x, y \in \mathbf{R}, \; x A y \iff |x| = |y|.$$

H 26. D is the relation defined on $\mathbf{Z}$ as follows: For every $m, n \in \mathbf{Z}$,

$$m D n \iff 3 \mid (m^2 - n^2).$$

27. R is the relation defined on $\mathbf{Z}$ as follows: For every $(m, n) \in \mathbf{Z}$,

$$m R n \iff 4 \mid (m^2 - n^2).$$

28. I is the relation defined on $\mathbf{R}$ as follows:

$$\text{For every } x, y \in \mathbf{R}, \quad m I n \iff x - y \text{ is an integer.}$$

29. Define P on the set $\mathbf{R} \times \mathbf{R}$ of ordered pairs of real numbers as follows: For every $(w, x), (y, z) \in \mathbf{R} \times \mathbf{R}$,

$$(w, x) P (y, z) \iff w = y.$$

30. Define Q on the set $\mathbf{R} \times \mathbf{R}$ as follows: For every $(w, x), (y, z) \in \mathbf{R} \times \mathbf{R}$,

$$(w, x) Q (y, z) \iff x = z.$$

31. Let P be the set of all points in the Cartesian plane except the origin. R is the relation defined on P as follows: For every p_1 and p_2 in P,

$$p_1 R p_2 \iff p_1 \text{ and } p_2 \text{ lie on the same half-line emanating from the origin.}$$

32. Let A be the set of all straight lines in the Cartesian plane. Define a relation $\parallel$ on A as follows:

For every l_1 and l_2 in A,

$$l_1 \parallel l_2 \iff l_1 \text{ is parallel to } l_2.$$

Then $\parallel$ is an equivalence relation on A. Describe the equivalence classes of this relation.

33. Let A be the set of points in the rectangle with x and y coordinates between 0 and 1. That is,

$$A = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid 0 \le x \le 1 \quad \text{and} \quad 0 \le y \le 1\}.$$

Define a relation R on A as follows: For all (x_1, y_1) and (x_2, y_2) in A,

$$\begin{aligned}(x_1, y_1) R (x_2, y_2) \iff & \\ & (x_1, y_1) = (x_2, y_2); \quad \text{or} \\ & x_1 = 0 \quad \text{and} \quad x_2 = 1 \quad \text{and} \quad y_1 = y_2; \quad \text{or} \\ & x_1 = 1 \quad \text{and} \quad x_2 = 0 \quad \text{and} \quad y_1 = y_2; \quad \text{or} \\ & y_1 = 0 \quad \text{and} \quad y_2 = 1 \quad \text{and} \quad x_1 = x_2; \quad \text{or} \\ & y_1 = 1 \quad \text{and} \quad y_2 = 0 \quad \text{and} \quad x_1 = x_2.\end{aligned}$$

In other words, all points along the top edge of the rectangle are related to the points along the bottom edge directly beneath them, and all points directly opposite each other along the left and right edges are related to each other. The points in the interior of the rectangle are not related to anything other than themselves. Then R is an equivalence relation on A. Imagine gluing together all the points that are in the same equivalence class. Describe the resulting figure.

34. The documentation for the computer language Java recommends that when an "equals method" is defined for an object, it be an equivalence relation. That is, if R is defined as follows:

$$x R y \iff x.equals(y) \quad \text{for all objects in the class,}$$

then R should be an equivalence relation. Suppose that in trying to optimize some of the mathematics of a graphics application, a programmer creates an object called a point, consisting of two coordinates in the plane. The programmer defines an equals method as follows: If p and q are any points, then

$$p.equals(q) \iff \text{the distance from } p \text{ to } q \text{ is less than or equal to } c$$

where c is a small positive number that depends on the resolution of the computer display. Is the

programmer's equals method an equivalence relation? Justify your answer.

35. Find an additional representative circuit for the input/output table of Example 8.3.9.

Let R be an equivalence relation on a set A. Prove each of the statements in 36–41 directly from the definitions of equivalence relation and equivalence class without using the results of Lemma 8.3.2, Lemma 8.3.3, or Theorem 8.3.4.

36. For every a in A, $a \in [a]$.

37. For every a and b in A, if $b \in [a]$ then $a \; R \; b$.

38. For every a, b, and c in A, if $b \; R \; c$ and $c \in [a]$ then $b \in [a]$.

39. For every a and b in A, if $[a] = [b]$ then $a \; R \; b$.

40. For every a, b, and x in A, if $a \; R \; b$ and $x \in [a]$ then $x \in [b]$.

H 41. For every a and b in A, if $a \in [b]$ then $[a] = [b]$.

42. Let R be the relation defined in Example 8.3.12.
- **a.** Prove that R is reflexive.
- **b.** Prove that R is symmetric.
- **c.** List four distinct elements in $[(1, 3)]$.
- **d.** List four distinct elements in $[(2, 5)]$.

*** 43.** In Example 8.3.12, define operations of addition $(+)$ and multiplication $(\cdot)$ as follows: For every $(a, b), (c, d) \in A$,

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$
$$[(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

- **a.** Prove that this addition is well defined. That is, show that if $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$, then $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$.
- **b.** Prove that this multiplication is well defined. That is, show that if $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$, then $[(ac, bd)] = [(a'c', b'd')]$.
- **c.** Show that $[(0, 1)]$ is an identity element for addition. That is, show that for any $(a, b) \in A$,

$$[(a, b)] + [(0, 1)] = [(0, 1)] + [(a, b)] = [(a, b)].$$

- **d.** Find an identity element for multiplication. That is, find (i, j) in A so that for every (a, b) in A, $[(a, b)] \cdot [(i, j)] = [(i, j)] \cdot [(a, b)] = [(a, b)]$.
- **e.** For any $(a, b) \in A$, show that $[(-a, b)]$ is an inverse for $[(a, b)]$ for addition. That is, show that $[(-a, b)] + [(a, b)] = [(a, b)] + [(-a, b)] = [(0, 1)]$.
- **f.** Given any $(a, b) \in A$ with $a \neq 0$, find an inverse for $[(a, b)]$ for multiplication. That is, find (c, d) in A so that $[(a, b)] \cdot [(c, d)] = [(c, d)] \cdot [(a, b)] = [(i, j)]$, where $[(i, j)]$ is the identity element you found in part (d).

44. Let $A = \mathbf{Z}^+ \times \mathbf{Z}^+$. Define a relation R on A as follows: For every (a, b) and (c, d) in A,

$$(a, b) \; R \; (c, d) \iff a + d = c + b.$$

- **a.** Prove that R is reflexive.
- **b.** Prove that R is symmetric.
- **H c.** Prove that R is transitive.
- **d.** List five elements in $[(1, 1)]$.
- **e.** List five elements in $[(3, 1)]$.
- **f.** List five elements in $[(1, 2)]$.
- **g.** Describe the distinct equivalence classes of R.

45. The following argument claims to prove that the requirement that an equivalence relation be reflexive is redundant. In other words, it claims to show that if a relation is symmetric and transitive, then it is reflexive. Find the mistake in the argument.

"**Proof:** Let R be a relation on a set A and suppose R is symmetric and transitive. For any two elements x and y in A, if $x \; R \; y$ then $y \; R \; x$ since R is symmetric. Thus it follows by transitivity that $x \; R \; x$, and hence R is reflexive."

46. Let R be a relation on a set A and suppose R is symmetric and transitive. Prove the following: If for every x in A there is a y in A such that $x \; R \; y$, then R is an equivalence relation.

47. Refer to the quote at the beginning of this section to answer the following questions.
- **a.** What is the name of the Knight's song called?
- **b.** What is the name of the Knight's song?
- **c.** What is the Knight's song called?
- **d.** What *is* the Knight's song?
- **e.** What is your (full, legal) name?
- **f.** What are you called?
- **g.** What *are* you? (Do not answer this on paper; just think about it.)

ANSWERS FOR TEST YOURSELF

1. reflexive, symmetric, and transitive **2.** m is congruent to n modulo d; d divides $m - n$ **3.** $[a]$; the set of all elements x in A such that $x \; R \; a$ **4.** $[a] \cap [b] = \varnothing$ **5.** a partition of A **6.** rational number

8.4 Modular Arithmetic with Applications to Cryptography

The "real" mathematics of the "real" mathematicians, the mathematics of Fermat and Euler and Gauss and Abel and Riemann, is almost wholly "useless." . . . It is not possible to justify the life of any genuine professional mathematician on the ground of the "utility" of his work. —G. H. Hardy, *A Mathematician's Apology*, 1941

Cryptography is the study of methods for sending secret messages. It involves **encryption**, in which a message, called **plaintext**, is converted into a form, called **ciphertext**, that is sent over a channel possibly open to view by outside parties. The receiver of the ciphertext uses **decryption** to convert the ciphertext back into plaintext.

With the rise of electronic communication systems, especially the Internet, the most important current use of cryptography is to enable transmission of confidential information, such as banking data, medical records, credit card numbers, and governmental communications, over electronic channels. Developing products for encryption and decryption is one of the main activities of the National Security Agency, which is the largest employer of mathematicians in the United States.

Many systems for sending secret messages require both the sender and the receiver to know both the encryption and the decryption procedures. For instance, an encryption system once used by Julius Caesar, and now called the **Caesar cipher**, encrypts messages by changing each letter of the alphabet to the one three places farther along, with X wrapping around to A, Y to B, and Z to C. In other words, say each letter of the alphabet is coded by its position relative to the others—so that A = 01, B = 02, . . . , Z = 26. If the numerical version of the plaintext for a letter is denoted M and the numeric version of the ciphertext is denoted C, then

$$C = (M + 3) \bmod 26.$$

The receiver of such a message can easily decrypt it by using the formula

$$M = (C - 3) \bmod 26.$$

For reference, here are the letters of the alphabet, together with their numeric equivalents:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 8.4.1 **Encrypting and Decrypting with the Caesar Cipher**

a. Use the Caesar cipher to encrypt the message HOW ARE YOU.

b. Use the Caesar cipher to decrypt the message L DP ILQH.

Solution

a. First, translate the letters of HOW ARE YOU into their numeric equivalents:

08 15 23 01 18 05 25 15 21.

Next, encrypt the message by adding 3 to each number. The result is

11 18 26 04 21 08 02 18 24.

Finally, substitute the letters that correspond to these numbers. The encrypted message becomes

KRZ DUH BRX.

b. First, translate the letters of L DP ILQH into their numeric equivalents:

12 04 16 09 12 17 08.

Next, decrypt the message by subtracting 3 from each number:

09 01 13 06 09 14 05.

Then, translate back into letters to obtain the original message: I AM FINE. ■

One problem with the Caesar cipher is that given a sufficient amount of ciphertext a person with knowledge of letter frequencies in the language can easily figure out the cipher. Partly for this reason, even Caesar himself did not make extensive use of it. Another problem with a system like the Caesar cipher is that knowledge of how to encrypt a message automatically gives knowledge of how to decrypt it. When a potential recipient of messages passes the encryption information to a potential sender of messages, the channel over which the information is passed may itself be insecure. Thus the information may leak out, enabling an outside party to decrypt messages intended to be kept secret.

With public-key cryptography, a potential recipient of encrypted messages openly distributes a public key containing the encryption information. However, knowledge of the public key provides virtually no clue about how messages are decrypted. Only the recipient has that knowledge. Regardless of how many people learn the encryption information, only the recipient should be able to decrypt messages that are sent.

The first public-key cryptography system was developed in 1976–1977 by three mathematician/computer scientists working at M.I.T.: Ronald Rivest, Adi Shamir, and

Kim Kulish/Getty Images

From left to right: Ronald Rivest (born 1948), Adi Shamir (born 1952), and Leonard Adleman (born 1945)

Leonard Adleman. In their honor it is called the RSA cipher. In order for you to learn how it works, you need to know some additional properties of congruence modulo n.

Properties of Congruence Modulo n

The first theorem in this section brings together a variety of equivalent ways of expressing the same basic arithmetic fact. Sometimes one way is most convenient; sometimes another way is best. You need to be comfortable moving from one to another, depending on the nature of the problem you are trying to solve.

Theorem 8.4.1 Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (nonnegative) remainder when divided by n
5. $a \bmod n = b \bmod n$

Proof: We will show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (1). It will follow by the transitivity of if-then that all five statements are equivalent.

So let a, b, and n be any integers with $n > 1$.

***Proof that* (1) $\Rightarrow$ (2):** Suppose that $n \mid (a - b)$. By definition of congruence modulo n, we can immediately conclude that $a \equiv b \pmod{n}$.

***Proof that* (2) $\Rightarrow$ (3):** Suppose that $a \equiv b \pmod{n}$. By definition of congruence modulo n, $n \mid (a - b)$. Thus, by definition of divisibility, $a - b = kn$, for some integer k. Adding b to both sides gives that $a = b + kn$.

***Proof that* (3) $\Rightarrow$ (4):** Suppose that $a = b + kn$, for some integer k. Use the quotient-remainder theorem to divide a by n to obtain

$$a = qn + r \quad \text{where } q \text{ and } r \text{ are integers and } 0 \leq r < n.$$

So r is the remainder obtained when a is divided by n. Substituting $b + kn$ for a in the equation $a = qn + r$ gives that

$$b + kn = qn + r,$$

and subtracting kn from both sides and factoring out n yields

$$b = (q - k)n + r.$$

Now since $0 \leq r < n$, the uniqueness property of the quotient-remainder theorem guarantees that r is also the remainder obtained when b is divided by n. Thus a and b have the same remainder when divided by n.

***Proof that* (4) $\Rightarrow$ (5):** Suppose that a and b have the same remainder when divided by n. It follows immediately from the definition of the *mod* function that $a \bmod n = b \bmod n$.

***Proof that* (5) ⇒ (1):** Suppose that $a \bmod n = b \bmod n$. By definition of the *mod* function, a and b have the same remainder when divided by n. Thus, by the quotient-remainder theorem, we can write

$$a = q_1 n + r \quad \text{and} \quad b = q_2 n + r \quad \text{where } q_1, q_2, \text{ and } r \text{ are integers and } 0 \le r < n.$$

It follows that

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n.$$

Therefore, since $q_1 - q_2$ is an integer, $n \mid (a - b)$.

Another consequence of the quotient-remainder theorem is this: When an integer a is divided by a positive integer n, a unique quotient q and remainder r are obtained with the property that $a = nq + r$ and $0 \le r < n$. Because there are exactly n integers that satisfy the inequality $0 \le r < n$ (the numbers from 0 through $n - 1$), there are exactly n possible remainders that can occur. These are called the *least nonnegative residues modulo n* or simply the *residues modulo n*.

Definition

Given integers a and n with $n > 1$, **the residue of *a* modulo *n*** is $a \bmod n$, the nonnegative remainder obtained when a is divided by n. The numbers $0, 1, 2, \ldots, n - 1$ are called a **complete set of residues modulo *n***. To **reduce a number modulo *n*** means to set it equal to its residue modulo n. If a modulus $n > 1$ is fixed throughout a discussion and an integer a is given, the words "modulo n" are often dropped and we simply speak of **the residue of *a***.

The following theorem generalizes several examples from Section 8.3.

Theorem 8.4.2 Congruence Modulo *n* Is an Equivalence Relation

If n is any integer with $n > 1$, congruence modulo n is an equivalence relation on the set of all integers. The distinct equivalence classes of the relation are the sets $[0], [1], [2], \ldots, [n - 1]$, where for each $a = 0, 1, 2, \ldots, n - 1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod{n}\},$$

or, equivalently,

$$[a] = \{m \in Z \mid m = a + kn \text{ for some integer } k\}.$$

Proof: Suppose n is any integer with $n > 1$. We must show that congruence modulo n is reflexive, symmetric, and transitive.

***Proof of reflexivity*:** Suppose a is any integer. To show that $a \equiv a \pmod{n}$, we must show that $n \mid (a - a)$. Now $a - a = 0$, and $n \mid 0$ because $0 = n \cdot 0$. Therefore $a \equiv a \pmod{n}$.

***Proof of symmetry*:** Suppose a and b are any integers such that $a \equiv b \pmod{n}$. We must show that $b \equiv a \pmod{n}$. Now since $a \equiv b \pmod{n}$, then $n \mid (a - b)$. Thus, by

(continued on page 528)

definition of divisibility, $a - b = nk$, for some integer k. Multiply both sides of this equation by -1 to obtain

$$-(a - b) = -nk,$$

or, equivalently,

$$b - a = n(-k).$$

Thus, by definition of divisibility $n \mid (b - a)$, and so, by definition of congruence modulo n, $b \equiv a \pmod{n}$.

***Proof of transitivity*:** This is left as exercise 5 at the end of the section.

***Proof that the distinct equivalence classes are* [0], [1], [2], . . . , [n − 1]:** This is left as exercise 6 at the end of the section.

Observe that there is a one-to-one correspondence between the distinct equivalence classes for congruence modulo n and the elements of a complete set of residues modulo n.

Modular Arithmetic

A fundamental fact about congruence modulo n is that if you first perform an addition, subtraction, or multiplication on integers and then reduce the result modulo n, you will obtain the same answer as if you had first reduced each of the numbers modulo n, performed the operation, and then reduced the result modulo n. For instance, instead of computing

$$(5 \cdot 8) = 40 \equiv 1 \pmod{3}$$

you will obtain the same answer if you compute

$$(5 \textit{ mod } 3)\,(8 \textit{ mod } 3) = 2 \cdot 2 = 4 \equiv 1 \pmod{3}.$$

The fact that this process works is a result of the following theorem.

Theorem 8.4.3 Modular Arithmetic

Let a, b, c, d, and n be integers with $n > 1$, and suppose

$$a \equiv c \pmod{n} \quad \text{and} \quad b \equiv d \pmod{n}.$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ for every positive integer m.

Proof: Because we will make greatest use of part 3 of this theorem, we prove it here and leave the proofs of the remaining parts of the theorem to exercises 9–11 at the end of the section.

***Proof of Part 3*:** Suppose a, b, c, d, and n are integers with $n > 1$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By Theorem 8.4.1, there exist integers s and t such that

$$a = c + sn \quad \text{and} \quad b = d + tn.$$

Then

$$\begin{aligned} ab &= (c + sn)(d + tn) && \text{by substitution} \\ &= cd + ctn + snd + sntn \\ &= cd + n(ct + sd + stn) && \text{by algebra.} \end{aligned}$$

Let $k = ct + sd + stn$. Then k is an integer because it is a sum of products of integers, and $ab = cd + nk$. Thus by Theorem 8.4.1, $ab \equiv cd \pmod{n}$.

Example 8.4.2 **Getting Started with Modular Arithmetic**

The most practical use of modular arithmetic is to reduce computations involving large integers to computations involving smaller ones. For instance, note that $55 \equiv 3 \pmod{4}$ because $55 - 3 = 52$, which is divisible by 4, and $26 \equiv 2 \pmod{4}$ because $26 - 2 = 24$, which is also divisible by 4. Verify the following statements.

a. $55 + 26 \equiv (3 + 2) \pmod{4}$ b. $55 - 26 \equiv (3 - 2) \pmod{4}$

c. $55 \cdot 26 \equiv (3 \cdot 2) \pmod{4}$ d. $55^2 \equiv 3^2 \pmod{4}$

Solution

a. Compute $55 + 26 = 81$ and $3 + 2 = 5$. By definition of congruence modulo n, to show that $81 \equiv 5 \pmod{4}$, you need to show that $4 \mid (81 - 5)$. But this is true because $81 - 5 = 76$, and $4 \mid 76$ since $76 = 4 \cdot 19$.

b. Compute $55 - 26 = 29$ and $3 - 2 = 1$. By definition of congruence modulo n, to show that $29 \equiv 1 \pmod{4}$, you need to show that $4 \mid (29 - 1)$. But this is true because $29 - 1 = 28$, and $4 \mid 28$ since $28 = 4 \cdot 7$.

c. Compute $55 \cdot 26 = 1430$ and $3 \cdot 2 = 6$. By definition of congruence modulo n, to show that $1430 \equiv 6 \pmod{4}$, you need to show that $4 \mid (1430 - 6)$. But this is true because $1430 - 6 = 1424$, and $4 \mid 1424$ since $1424 = 4 \cdot 356$.

d. Compute $55^2 = 3025$ and $3^2 = 9$. By definition of congruence modulo n, to show that $3025 \equiv 9 \pmod{4}$, you need to show that $4 \mid (3025 - 9)$. But this is true because $3025 - 9 = 3016$, and $4 \mid 3016$ since $3016 = 4 \cdot 754$. ■

In order to facilitate the computations performed in this section, it is convenient to express part 3 of Theorem 8.4.3 in a slightly differently form.

Corollary 8.4.4

Let a, b, and n be integers with $n > 1$. Then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$

Example 8.4.3 **Computing a Product Modulo *n***

As in Example 8.4.2, note that $55 \equiv 3 \pmod 4$ and $26 \equiv 2 \pmod 4$. Because both 3 and 2 are less than 4, each of these numbers is a least nonnegative residue modulo 4. Therefore, $55 \bmod 4 = 3$ and $26 \bmod 4 = 2$. Use the notation of Corollary 8.4.4 to find the residue of $55 \cdot 26$ modulo 4.

Solution Recall that to use a calculator to compute remainders, you can use the formula $n \bmod d = n - d \cdot \lfloor n/d \rfloor$. If you are using a hand calculator with an "integer part" feature and both n and d are positive, then $\lfloor n/d \rfloor$ is the integer part of the division of n by d. When you divide a positive integer n by a positive integer d with a more basic calculator, you can see $\lfloor n/d \rfloor$ on the calculator display by simply ignoring the digits that follow the decimal point.

By Corollary 8.4.4,

$$\begin{aligned}(55 \cdot 26) \bmod 4 &= \{(55 \bmod 4)(26 \bmod 4)\} \bmod 4 \\ &\equiv (3 \cdot 2) \bmod 4 && \text{because } 55 \bmod 4 = 3 \text{ and } 26 \bmod 4 = 2 \\ &\equiv 6 \bmod 4 \\ &\equiv 2 && \text{because } 4 \mid (6-2) \text{ and } 2 < 4.\end{aligned}$$

■

When modular arithmetic is performed with very large numbers, as is the case for RSA crytography, computations are facilitated by using two properties of exponents. The first is

$$x^{2a} = (x^a)^2 \quad \text{for all real numbers } x \text{ and } a \text{ with } x \geq 0. \tag{8.4.1}$$

Thus, for instance, if x is any positive real number, then

$$\begin{aligned}x^4 \bmod n &= (x^2)^2 \bmod n && \text{because } (x^2)^2 = x^4 \\ &= (x^2 \bmod n)^2 \bmod n && \text{by Corollary 8.4.4.}\end{aligned}$$

Hence you can reduce x^4 modulo n by reducing x^2 modulo n and then reducing the square of the result modulo n. Because all the residues are less than n, this process limits the size of the computations to numbers that are less than n^2, which makes them easier to work with, both for humans (when the numbers are relatively small) and for computers (when the numbers are very large).

A second useful property of exponents is

$$x^{a+b} = x^a x^b \quad \text{for all real numbers } x, a, \text{ and } b \text{ with } x \geq 0. \tag{8.4.2}$$

For instance, because $7 = 4 + 2 + 1$,

$$x^7 = x^4 x^2 x^1.$$

Thus, by Corollary 8.4.4,

$$x^7 \bmod n = \{(x^4 \bmod n)(x^2 \bmod n)(x^1 \bmod n)\} \bmod n.$$

We first show an example that illustrates the application of formula (8.4.1) and then an example that uses both (8.4.1) and (8.4.2).

Example 8.4.4 **Computing $a^k \bmod n$ When k Is a Power of 2**

Find $144^4 \bmod 713$.

Solution Use property (8.4.1) to write $144^4 = (144^2)^2$. Then

$$\begin{aligned}
144^4 \bmod 713 &= (144^2)^2 \bmod 713 \\
&= (144^2 \bmod 713)^2 \bmod 713 \\
&= (20736 \bmod 713)^2 \bmod 713 && \text{because } 144^2 = 20736 \\
&= 59^2 \bmod 713 && \text{because } 20736 \bmod 713 = 59 \\
&= 3481 \bmod 713 && \text{because } 59^2 = 3481 \\
&= 629 && \text{because } 3481 \bmod 713 = 629.
\end{aligned}$$

■

Example 8.4.5 **Computing $a^k \bmod n$ When k Is Not a Power of 2**

Find $12^{43} \bmod 713$.

Solution First write the exponent as a sum of powers of 2:

$$43 = 2^5 + 2^3 + 2 + 1 = 32 + 8 + 2 + 1.$$

Next compute 12^{2^k} for $k = 0, 1, 2, 3, 4$, and 5.

$$\begin{aligned}
12 \bmod 713 &= 12 \\
12^2 \bmod 713 &= 144 \\
12^4 \bmod 713 &= 144^2 \bmod 713 = 59 && \text{by Example 8.4.4} \\
12^8 \bmod 713 &= 59^2 \bmod 713 = 629 && \text{by Example 8.4.4} \\
12^{16} \bmod 713 &= 629^2 \bmod 713 = 639 && \text{by the method of Example 8.4.4} \\
12^{32} \bmod 713 &= 639^2 \bmod 713 = 485 && \text{by the method of Example 8.4.4.}
\end{aligned}$$

By property (8.4.2),

$$12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1.$$

Thus, by Corollary 8.4.4,

$$\begin{aligned}
&12^{43} \bmod 713 \\
&\quad = \{(12^{32} \bmod 713) \cdot (12^8 \bmod 713) \cdot (12^2 \bmod 713) \cdot (12 \bmod 713)\} \bmod 713.
\end{aligned}$$

By substitution,

$$\begin{aligned}
12^{43} \bmod 713 &= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 \\
&= 527152320 \bmod 713 \\
&= 48.
\end{aligned}$$

■

You should know how to do the computations in Example 8.4.5 by hand using only a simple electronic calculator, but if you are computing a lot of residues, especially ones involving large numbers, you may want to write a short computer or calculator program to do the computations for you.

Extending the Euclidean Algorithm

An extended version of the Euclidean algorithm can be used to find a concrete expression for the greatest common divisor of integers a and b.

Definition

An integer d is said to be a **linear combination of integers** a and b if, and only if, there exist integers s and t such that $as + bt = d$.

Theorem 8.4.5 Writing a Greatest Common Divisor as a Linear Combination

For all integers a and b, not both zero, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Proof: Given integers a and b, not both zero, and given $d = \gcd(a, b)$, let

$$S = \{x \mid x \text{ is a positive integer and } x = as + bt \text{ for some integers } s \text{ and } t\}.$$

Note that S is a nonempty set because (1) if $a > 0$ then $1 \cdot a + 0 \cdot b \in S$, (2) if $a < 0$ then $(-1) \cdot a + 0 \cdot b \in S$, and (3) if $a = 0$ then, by assumption, $b \neq 0$, and hence $0 \cdot a + 1 \cdot b \in S$ or $0 \cdot a + (-1) \cdot b \in S$. Thus, because S is a nonempty subset of positive integers, by the well-ordering principle for the integers there is a least element c in S. By definition of S,

$$c = as + bt \quad \text{for some integers } s \text{ and } t. \tag{8.4.3}$$

We will show that (1) $c \geq d$, and (2) $c \leq d$, and we will therefore be able to conclude that $c = d = \gcd(a, b)$.

(1) *Proof that $c \geq d$*:
[In this part of the proof, we show that d is a divisor of c and thus that $d \leq c$.] Because $d = \gcd(a, b)$, by definition of greatest common divisor, $d \mid a$ and $d \mid b$. Hence $a = dx$ and $b = dy$ for some integers x and y. Then

$$\begin{aligned} c &= as + bt && \text{by (8.4.3)} \\ &= (dx)s + (dy)t && \text{by substitution} \\ &= d(xs + y) && \text{by factoring out the } d. \end{aligned}$$

Now $xs + yt$ is an integer because it is a sum of products of integers. Thus, by definition of divisibility, $d \mid c$. Both c and d are positive, and hence, by Theorem 4.4.1, $c \geq d$.

(2) *Proof that $c \leq d$*:
[In this part of the proof, we show that c is a divisor of both a and b and therefore that c is less than or equal to the greatest common divisor of a and b, which is d.] Apply the quotient-remainder theorem to the division of a by c to obtain

$$a = cq + r \quad \text{for some integers } q \text{ and } r \text{ with } 0 \leq r < c. \tag{8.4.4}$$

Thus for some integers q and r with $0 \leq r < c$,

$$r = a - cq.$$

Now $c = as + bt$. Therefore, for some integers q and r with $0 \leq r < c$,

$$\begin{aligned} r &= a - (as + bt)q && \text{by substitution.} \\ &= a(1 - sq) - btq \end{aligned}$$

Thus r is a linear combination of a and b. If $r > 0$, then r would be in S, and so r would be a smaller element of S than c, which would contradict the fact that c is the least element of S. Hence $r = 0$. By substitution into (8.4.4),

$$a = cq$$

and therefore $c \mid a$.

An almost identical argument establishes that $c \mid b$ and is left as exercise 30 at the end of the section.

Because $c \mid a$ and $c \mid b$, c is a common divisor of a and b. Hence c is less than or equal to the greatest common divisor of a and b. In other words, $c \leq d$.

From (1) and (2), we conclude that $c = d$. It follows that d, the greatest common divisor of a and b, is equal to $as + bt$.

The following example shows a practical method for expressing the greatest common divisor of two integers as a linear combination of the two.

Example 8.4.6 **Expressing a Greatest Common Divisor as a Linear Combination**

In Example 4.10.6 we showed how to use the Euclidean algorithm to find that the greatest common divisor of 330 and 156 is 6. Use the results of those calculations to express gcd(330, 156) as a linear combination of 330 and 156.

Solution The first four steps of the solution restate and extend results from Example 4.10.6, which were obtained by successive applications of the quotient-remainder theorem. The fifth step shows how to find the coefficients of the linear combination by substituting back through the results of the previous steps.

Step 1: $330 = 156 \cdot 2 + 18$, which implies that $18 = 330 - 156 \cdot 2$.

Step 2: $156 = 18 \cdot 8 + 12$, which implies that $12 = 156 - 18 \cdot 8$.

Step 3: $18 = 12 \cdot 1 + 6$, which implies that $6 = 18 - 12 \cdot 1$.

Step 4: $12 = 6 \cdot 2 + 0$, which implies that $\gcd(330, 156) = 6$.

Step 5: By substituting back through steps 3 to 1:

$$\begin{aligned}
6 &= 18 - 12 \cdot 1 && \text{from step 3} \\
&= 18 - (156 - 8 \cdot 18) \cdot 1 && \text{by substitution from step 2} \\
&= 9 \cdot 18 + (-1) \cdot 156 && \text{by algebra} \\
&= 9 \cdot (330 - 156 \cdot 2) + (-1) \cdot 156 && \text{by substitution from step 1} \\
&= 9 \cdot 330 + (-19) \cdot 156 && \text{by algebra.}
\end{aligned}$$

Thus $\gcd(330, 156) = 9 \cdot 330 + (-19) \cdot 156$. (It is always a good idea to check the result of a calculation like this to be sure you did not make a mistake. In this case, you find that $9 \cdot 330 + (-19) \cdot 156$ does indeed equal 6.) ■

The Euclidean algorithm given in Section 4.10 can be adapted so as to compute the coefficients of the linear combination of the gcd at the same time as it computes the gcd itself. This extended Euclidean algorithm is described in the exercises at the end of the section.

Finding an Inverse Modulo n

Suppose you want to solve the following congruence for x:

$$2x \equiv 3 \pmod 5.$$

Note that $3 \cdot 2 = 6 \equiv 1 \pmod 5$. So 3 appears to be a kind of inverse for 2 modulo 5. Thus multiplying both sides of the congruence to be solved by 3 might give a solution for x. When we try this, we obtain

$$6x = 3 \cdot 2x \equiv 3 \cdot 3 \pmod 5 \equiv 9 \pmod 5 \equiv 4 \pmod 5.$$

Now since $6 \equiv 1 \pmod 5$, Theorem 8.4.3(3) implies that

$$6x \equiv 1 \cdot x \pmod 5 \equiv x \pmod 5.$$

So, $6x \equiv 4 \pmod 5$ and $6x \equiv x \pmod 5$, and, hence, by the symmetric and transitive properties of modular congruence,

$$x \equiv 4 \pmod 5.$$

Therefore, a solution is $x = 4$. (You can check that $2 \cdot 4 = 8 \equiv 3 \pmod 5$.)

Definition

Given any integer a and any positive integer n, if there exists an integer s such that $as \equiv 1 \pmod n$, then s is called **an inverse for a modulo n**.

Unfortunately, the method shown above cannot always be used to solve congruences because not every integer has an inverse modulo n. For instance, observe that

$$2 \cdot 1 \equiv 2 \pmod 4$$
$$2 \cdot 2 \equiv 0 \pmod 4$$
$$2 \cdot 3 \equiv 2 \pmod 4.$$

By Theorem 8.4.3, these calculations suffice to show that the number 2 does not have an inverse modulo 4.

Describing the circumstances in which inverses exist in modular arithmetic requires the concept of relative primeness.

Definition

Integers a and b are **relatively prime** if, and only if, $\gcd(a, b) = 1$. Integers $a_1, a_2, a_3, \ldots, a_n$ are **pairwise relatively prime** if, and only if, $\gcd(a_i, a_j) = 1$ for all integers i and j with $1 \le i, j \le n$, and $i \ne j$.

Given the definition of relatively prime integers, the following corollary is an immediate consequence of Theorem 8.4.5.

Corollary 8.4.6

If a and b are relatively prime integers, then there exist integers s and t such that $as + bt = 1$.

Example 8.4.7 **Expressing 1 as a Linear Combination of Relatively Prime Integers**

Show that 660 and 43 are relatively prime, and find a linear combination of 660 and 43 that equals 1.

Solution

Step 1: Divide 660 by 43 to obtain $660 = 43 \cdot 15 + 15$, which implies that $15 = 660 - 43 \cdot 15$.

Step 2: Divide 43 by 15 to obtain $43 = 15 \cdot 2 + 13$, which implies that $13 = 43 - 15 \cdot 2$.

Step 3: Divide 15 by 13 to obtain $15 = 13 \cdot 1 + 2$, which implies that $2 = 15 - 13$.

Step 4: Divide 13 by 2 to obtain $13 = 2 \cdot 6 + 1$, which implies that $1 = 13 - 2 \cdot 6$.

Step 5: Divide 2 by 1 to obtain $2 = 1 \cdot 2 + 0$, which implies that $\gcd(660, 43) = 1$ and so 660 and 43 are relatively prime.

Step 6: To express 1 as a linear combination of 660 and 43, substitute back through steps 4 to 1:

$$\begin{aligned}
1 &= 13 - 2 \cdot 6 && \text{from step 4} \\
&= 13 - (15 - 13) \cdot 6 && \text{by substitution from step 3} \\
&= 7 \cdot 13 - 6 \cdot 15 && \text{by algebra} \\
&= 7 \cdot (43 - 15 \cdot 2) - 6 \cdot 15 && \text{by substitution from step 2} \\
&= 7 \cdot 43 - 20 \cdot 15 && \text{by algebra} \\
&= 7 \cdot 43 - 20 \cdot (660 - 43 \cdot 15) && \text{by substitution from step 1} \\
&= 307 \cdot 43 - 20 \cdot 660 && \text{by algebra.}
\end{aligned}$$

Thus $\gcd(660, 43) = 1 = 307 \cdot 43 - 20 \cdot 660$. (And a check by direct computation confirms that $307 \cdot 43 - 20 \cdot 660$ does indeed equal 1.) ■

A consequence of Corollary 8.4.6 is that under certain circumstances, it is possible to find an inverse for an integer modulo n.

Corollary 8.4.7 Existence of Inverses Modulo *n*

For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integer s such that $as \equiv 1 \pmod{n}$, and so s is an inverse for a modulo n.

Proof: Suppose a and n are integers and $\gcd(a, n) = 1$. By Corollary 8.4.6, there exist integers s and t such that

$$as + nt = 1.$$

Subtracting nt from both sides gives that

$$as = 1 - nt = 1 + (-t)n.$$

Thus, by definition of congruence modulo n,

$$as \equiv 1 \pmod{n}.$$

Example 8.4.8 **Finding an Inverse Modulo *n***

a. Find an inverse for 43 modulo 660. That is, find an integer s such that $43s \equiv 1 \pmod{660}$.

b. Find a positive inverse for 3 modulo 40. That is, find a positive integer s such that $3s \equiv 1 \pmod{40}$.

Solution

a. By Example 8.4.7,

$$307 \cdot 43 - 20 \cdot 660 = 1.$$

Adding $20 \cdot 660$ to both sides gives that

$$307 \cdot 43 = 1 + 20 \cdot 660.$$

Thus, by definition of congruence modulo 660,

$$307 \cdot 43 \equiv 1 \pmod{660},$$

so 307 is an inverse for 43 modulo 660.

b. Use the technique of Example 8.4.7 to find a linear combination of 3 and 40 that equals 1.

Step 1: Divide 40 by 3 to obtain $40 = 3 \cdot 13 + 1$. This implies that $1 = 40 - 3 \cdot 13$.

Step 2: Divide 3 by 1 to obtain $3 = 3 \cdot 1 + 0$. This implies that $\gcd(3, 40) = 1$.

Step 3: Use the result of step 1 to write

$$3 \cdot (-13) = 1 + (-1)40.$$

This result implies that -13 is an inverse for 3 modulo 40. In other words, $3 \cdot (-13) \equiv 1 \pmod{40}$. To find a positive inverse, compute $40 - 13$. The result is 27, and

$$27 \equiv -13 \pmod{40}$$

because $27 - (-13) = 40$. So, by Theorem 8.4.3(3),

$$3 \cdot 27 \equiv 3 \cdot (-13) \equiv 1 \pmod{40},$$

and thus by the transitive property of congruence modulo n, 27 is a positive integer that is an inverse for 3 modulo 40. ■

RSA Cryptography

At this point we have developed enough number theory to explain how to encrypt and decrypt messages using the RSA cipher. The effectiveness of the system is based on the fact that although modern computer algorithms make it quite easy to find two distinct large integers p and q—say on the order of several hundred digits each—that are virtually certain to be prime, even the fastest computers are not currently able to factor their product, an integer with approximately twice that many digits. In order to encrypt a message using the RSA cipher, a person needs to know the value of pq and of another integer e, both of which are made publicly available. But only a person who knows the individual values of p and q can decrypt an encrypted message.

We first give an example to show *how* the cipher works and then discuss some of the theory to explain *why* it works. The example is unrealistic in the sense that because p and q are so small, it would be easy to figure out what they are just by knowing

their product. But working with small numbers conveys the idea of the system, while keeping the computations in a range that can be performed with a hand calculator.

Suppose Alice decides to set up an RSA cipher. She chooses two prime numbers—say, $p = 5$ and $q = 11$—and computes $pq = 55$. She then chooses a positive integer e that is relatively prime to $(p - 1)(q - 1)$. In this case, $(p - 1)(q - 1) = 4 \cdot 10 = 40$, so she may take $e = 3$ because 3 is relatively prime to 40. (In practice, taking e to be small could compromise the secrecy of the cipher, so she would take a larger number than 3. However, the mathematics of the cipher works as well for 3 as for a larger number, and the smaller number makes for easier calculations.)

The number pair (pq, e) is Alice's **public key**, which she may distribute widely. Because the RSA cipher works only on numbers, Alice also informs people how she will interpret the numbers in the messages they send her. Let us suppose that she encodes letters of the alphabet in a similar way as was done for the Caesar cipher:

$$A = 01, B = 02, C = 03, \ldots, Z = 26.$$

Let us also assume that the messages Alice receives consist of blocks, each of which, for simplicity, is taken to be a single, numerically encoded letter of the alphabet.

Someone who wants to send Alice a message breaks the message into blocks, each consisting of a single letter, and finds the numeric equivalent for each block. The plaintext, M, in a block is converted into ciphertext, C, according to the following formula:

$$C = M^e \bmod pq. \tag{8.4.5}$$

Note that because (pq, e) is the public key, anyone who has it and knows modular arithmetic can encrypt a message to send to Alice.

Example 8.4.9 **Encrypting a Message Using RSA Cryptography**

Bob wants to send Alice the message HI. What is the ciphertext for his message?

Solution Bob will send his message in two blocks, one for the H and another for the I. Because H is the eighth letter in the alphabet, it is encoded as 08, or 8. The corresponding ciphertext is computed using formula 8.4.5 as follows:

$$\begin{aligned} C &= 8^3 \bmod 55 \\ &= 512 \bmod 55 \\ &= 17. \end{aligned}$$

Because I is the ninth letter in the alphabet, it is encoded as 09, or 9. The corresponding ciphertext is

$$\begin{aligned} C &= 9^3 \bmod 55 \\ &= 729 \bmod 55 \\ &= 14. \end{aligned}$$

Accordingly, Bob sends Alice the message: 17 14. ■

To decrypt the message, the *decryption key* must be computed. It is a number d that is a positive inverse to e modulo $(p - 1)(q - 1)$. The plaintext M is obtained from the ciphertext C by the formula

$$M = C^d \bmod pq, \text{ where the number pair } (pq, d) \text{ is Alice's } \textbf{private key}. \tag{8.4.6}$$

Note that because $M + kpq \equiv M \pmod{pq}$, M must be taken to be less than pq, as in the above example, in order for the decryption to be guaranteed to produce the original message. But because p and q are normally taken to be so large, this requirement does not cause problems. Long messages are broken into blocks of symbols to meet the restriction and several symbols are included in each block to prevent decryption based on knowledge of letter frequencies.

Example 8.4.10 **Decrypting a Message Using RSA Cryptography**

Imagine that Alice has hired you to help her decrypt messages and has shared with you the values of p and q. Compute Alice's private key (pq, d) and use the formula $M = C^d \bmod pq$ to decrypt the following ciphertext for her: 17 14.

Solution Because $p = 5$ and $q = 11$, $(p-1)(q-1) = 40$, the decryption key d is a positive inverse for 3 modulo 40. Knowing that you would need this number, we computed it in Example 8.4.8(b) and found it to be 27. Thus to decrypt the ciphertext 17, you need to compute

$$M = 17^d \bmod pq = 17^{27} \bmod 55.$$

To do so, note that

$$27 = 16 + 8 + 2 + 1.$$

Next, find the residues obtained when 17 is raised to successively higher powers of 2, up to $2^4 = 16$:

$$\begin{aligned}
17 \bmod 55 &= 17 \bmod 55 &&= 17\\
17^2 \bmod 55 &= 17^2 \bmod 55 &&= 14\\
17^4 \bmod 55 &= (17^2)^2 \bmod 55 = 14^2 \bmod 55 &&= 31\\
17^8 \bmod 55 &= (17^4)^2 \bmod 55 = 31^2 \bmod 55 &&= 26\\
17^{16} \bmod 55 &= (17^8)^2 \bmod 55 = 26^2 \bmod 55 &&= 16
\end{aligned}$$

Then use the fact that

$$17^{27} = 17^{16+8+2+1} = 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17^1$$

to write

$$\begin{aligned}
17^{27} \bmod 55 &= (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17) \bmod 55\\
&\equiv [(17^6 \bmod 55)(17^8 \bmod 55)(17^2 \bmod 55)(17 \bmod 55)] \pmod{55}\\
&\qquad \text{by Corollary 8.4.4}\\
&\equiv (16 \cdot 26 \cdot 14 \cdot 17) \pmod{55}\\
&\equiv 99008 \pmod{55}\\
&\equiv 8 \pmod{55}.
\end{aligned}$$

Hence $17^{27} \bmod 55 = 8$, and thus the plaintext of the first part of Bob's message is 8, or 08. In the last step, you find the letter corresponding to 08, which is *H*. In exercises 14 and 15 at the end of this section, you are asked to show that when you decrypt 14, the result is 9, which corresponds to the letter I, so you can tell Alice that Bob's message is HI. ■

Figure 8.4.1 illustrates the process of sending and receiving a message using RSA cryptography.

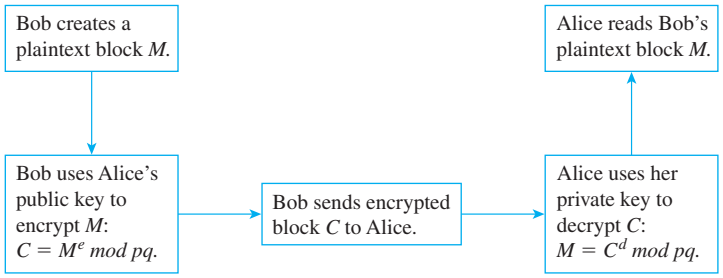


FIGURE 8.4.1 Using RSA cryptography

Euclid's Lemma

Another consequence of Theorem 8.4.5 is known as *Euclid's lemma*. It is the crucial fact behind the unique factorization theorem for the integers and is also of great importance in many other parts of number theory.

Theorem 8.4.8 Euclid's Lemma

For all integers a, b, and c, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

Proof: Suppose a, b, and c are integers, $\gcd(a, c) = 1$, and $a \mid bc$. *[We must show that* $a|b$*.]* By Theorem 8.4.5, there exist integers s and t so that

$$as + ct = 1.$$

Multiply both sides of this equation by b to obtain

$$bas + bct = b. \tag{8.4.7}$$

Since $a|bc$, by definition of divisibility there exists an integer k such that

$$bc = ak. \tag{8.4.8}$$

Substituting (8.4.8) into (8.4.7), rewriting, and factoring out an a gives that

$$b = bas + (ak)t = a(bs + kt).$$

Let $r = bs + kt$. Then r is an integer (because b, s, k, and t are all integers), and $b = ar$. Thus $a|b$ by definition of divisibility.

The unique factorization theorem for the integers states that any integer greater than 1 has a unique representation as a product of prime numbers, except possibly for the order in which the numbers are written. The hint for exercise 13 of Section 5.4 outlined a proof of the existence part of the proof, and the uniqueness of the representation follows quickly from Euclid's lemma. In exercise 41 at the end of this section, we outline a proof for you to complete.

Another application of Euclid's lemma is a cancellation theorem for congruence modulo n. This theorem allows us—under certain circumstances—to divide out a common factor in a congruence relation.

Theorem 8.4.9 Cancellation Theorem for Modular Congruence

For all integers a, b, c, and n with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

(continued on page 540)

Proof: Suppose a, b, c, and n are any integers, $\gcd(c, n) = 1$, and $ac \equiv bc \pmod{n}$. *[We must show that $a \equiv b$ (mod n).]* By definition of congruence modulo n,

$$n \mid (ac - bc),$$

and so, since

$$ac - bc = (a - b)c,$$

then

$$n \mid (a - b)c.$$

Because $\gcd(c, n) = 1$, we may apply Euclid's lemma to obtain

$$n \mid (a - b),$$

and so, by definition of congruence modulo n,

$$a \equiv b \pmod{n}.$$

An alternative proof for Theorem 8.4.9 uses Corollary 8.4.7. Because $\gcd(c, n) = 1$, the corollary guarantees an inverse for c modulo n. In the proof of Theorem 8.4.9, let d denote an inverse for c. Apply Theorem 8.4.3(3) repeatedly, first to multiply both sides of $ac \equiv bc \pmod{n}$ by d to obtain $(ac)d \equiv (bd)d \pmod{n}$, and then to use the fact that $cd \equiv 1 \pmod{n}$ to simplify the congruence and conclude that $a \equiv b \pmod{n}$.

Fermat's Little Theorem

Fermat's little theorem was given that name to distinguish it from Fermat's last theorem, which we discussed in Section 4.1. It provides the theoretical underpinning for RSA cryptography.

Theorem 8.4.10 Fermat's Little Theorem

If p is any prime number and a is any integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: Suppose p is any prime number and a is any integer such that $p \nmid a$. Note that $a \neq 0$ because otherwise p would divide a. Consider the set of integers

$$S = \{a, 2a, 3a, \ldots, (p - 1)a\}.$$

We claim that no two elements of S are congruent modulo p. For suppose $sa \equiv ra \pmod{p}$ for some integers s and r with $1 \leq r < s \leq p - 1$. Then, by definition of congruence modulo p,

$$p \mid (sa - ra), \quad \text{or, equivalently,} \quad p \mid (s - r)a.$$

Now $p \nmid a$ by hypothesis, and because p is prime, $\gcd(a, p) = 1$. Thus, by Euclid's lemma, $p \mid (s - r)$. But this is impossible because $0 < s - r < p$.

Consider the function F from S to the set $T = \{1, 2, 3, \ldots, (p - 1)\}$ that sends each element of S to its residue modulo p. Then F is one-to-one because no two elements of S are congruent modulo p. In Section 9.4 we prove that if a function from one finite set to another is one-to-one, then it is also onto. Hence F is onto, and so the $p - 1$ residues of the $p - 1$ elements of S are exactly the numbers $1, 2, 3, \ldots, (p - 1)$.

It follows by Theorem 8.4.3(3) that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv [1 \cdot 2 \cdot 3 \cdots (p-1)] \,(\text{mod}\, p),$$

or, equivalently,

$$a^{p-1}(p-1)! \equiv (p-1)! \,(\text{mod}\ p).$$

Now because p is prime, p and $(p-1)!$ are relatively prime. Thus, by the cancellation theorem for modular congruence (Theorem 8.4.9),

$$a^{p-1} \equiv 1 \,(\text{mod}\ p).$$

Why Does the RSA Cipher Work?

For the RSA cryptography method, the formula

$$M = C^d \ mod\ pq$$

is supposed to produce the original plaintext message, M, when the encrypted message is C. How can we be sure that it always does so? Recall that we require that $M < pq$, and we know that $C = M^e \ mod\ pq$. So, by substitution,

$$C^d \ mod\ pq = (M^e \ mod\ pq)^d \ mod\ pq.$$

By Theorem 8.4.3(4),

$$(M^e \ mod\ pq)^d \equiv M^{ed} \,(\text{mod}\ pq).$$

Thus $C^d \ mod\ pq \equiv M^{ed} \,(\text{mod}\ pq)$, and so it suffices to show that

$$M \equiv M^{ed} \,(\text{mod}\ pq).$$

Recall that d was chosen to be a positive inverse for e modulo $(p-1)(q-1)$, which exists because $\gcd(e, (p-1)(q-1)) = 1$. In other words,

$$ed \equiv 1 \,(\text{mod}\ (p-1)(q-1)),$$

or, equivalently,

$$ed = 1 + k(p-1)(q-1) \quad \text{for some positive integer } k.$$

Therefore,

$$M^{ed} = M^{1+k(p-1)(q-1)} = M(M^{k(p-1)(q-1)}).$$

If $p \nmid M$, then by Fermat's little theorem, $M^{p-1} \equiv 1 \,(\text{mod}\ p)$, and so

$$M^{ed} = M(M^{k(p-1)(q-1)}) = M(M^{p-1})^{k(q-1)} \equiv M(1)^{k(q-1)} \,(\text{mod}\ p) = M \,(\text{mod}\ p).$$

Similarly, if $q \nmid M$, then by Fermat's little theorem, $M^{q-1} \equiv 1 \,(\text{mod}\ q)$, and so

$$M^{ed} = M(M^{k(p-1)(q-1)}) = M(M^{q-1})^{k(p-1)} \equiv M(1)^{k(p-1)} \,(\text{mod}\ q) = M \,(\text{mod}\ q).$$

Thus, if M is relatively prime to pq,

$$M^{ed} \equiv M \,(\text{mod}\ p) \quad \text{and} \quad M^{ed} \equiv M \,(\text{mod}\ q).$$

If M is not relatively prime to pq, then either $p \mid M$ or $q \mid M$. If $p \mid M$, then $M^{ed} \equiv 0 \equiv M \pmod{p}$, and if $q \mid M$, then $M^{ed} \equiv 0 \equiv M \pmod{q}$. If $q \nmid M$, then as above, $M^{ed} \equiv M \pmod{q}$, and if $p \nmid M$, then as above, $M^{ed} \equiv M \pmod{p}$. Thus, in all cases,

$$M^{ed} \equiv M \pmod{p} \quad \text{and} \quad M^{ed} \equiv M \pmod{q}.$$

By Theorem 8.4.1,

$$p \mid (M^{ed} - M) \quad \text{and} \quad q \mid (M^{ed} - M),$$

and, by definition of divisibility,

$$M^{ed} - M = pt \text{ for some integer } t.$$

By substitution,

$$q \mid pt,$$

and since q and p are distinct prime numbers, Euclid's lemma applies to give

$$q \mid t.$$

Thus

$$t = qu \quad \text{for some integer } u$$

by definition of divisibility. By substitution,

$$M - M^{ed} = pt = p(qu) = (pq)u,$$

where u is an integer, and so,

$$pq \mid (M - M^{ed})$$

by definition of divisibility. Thus

$$M - M^{ed} \equiv 0 \pmod{pq}$$

by definition of congruence, or, equivalently,

$$M \equiv M^{ed} \pmod{pq}.$$

Because $M < pq$, this last congruence implies that

$$M = M^{ed} \; mod \; pq,$$

and thus the RSA cipher gives the correct result.

Message Authentication

In some Internet networks, such as those that use blockchain technology, individuals have their own public keys but their actual identities are private. Suppose Alice and Bob are part of the network, so each knows the other's public key. Alice wants to send Bob a message, but she has a problem. She wants to make sure that Bob will know that the message really is from her. After all everyone in the network has Bob's public key, and so someone else could send Bob a message pretending that it is from Alice.

The solution follows from the fact that in the formula $M = M^{ed} \; mod \; pq$, e and d are interchangeable. Alice can use her private key (pq, d) and the formula

$$M = M^{ed} \; mod \; pq$$

to encrypt some identifying information showing that she is the person she claims to be. Then she adds the encrypted information to her plaintext message for Bob and uses Bob's public key to encrypt the communication as a whole.

When Bob receives the communication, he uses his private key to decrypt it. He discovers that part is plaintext, claiming to be from Alice, and another part is encrypted. So he uses Alice's public key to decrypt the encrypted part and finds Alice's identifying information. He then knows the message is authentic because only Alice has the private key needed to perform the encryption.

This process of message authentication is illustrated in Figure 8.4.2.

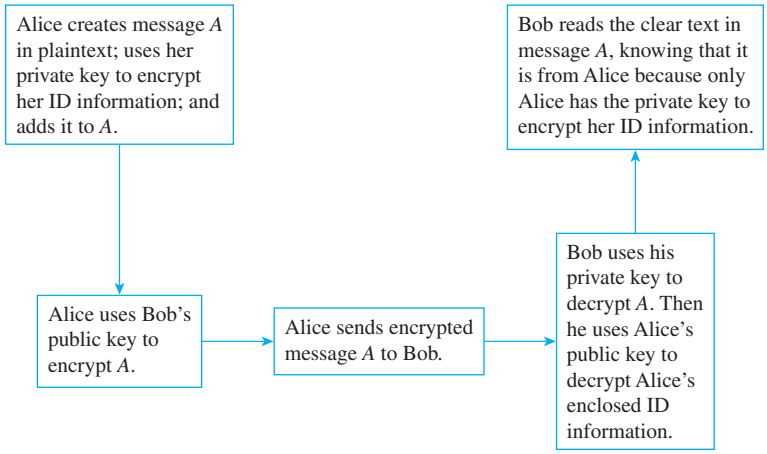


FIGURE 8.4.2 Message authentication

Additional Remarks on Number Theory and Cryptography

The famous British mathematician G. H. Hardy (1877–1947) was fond of comparing the beauty of pure mathematics, especially number theory, to the beauty of art. Indeed, the theorems in this section have many beautiful and striking consequences beyond those we have had the space to describe, and the subject of number theory extends far beyond these theorems. Hardy also enjoyed describing pure mathematics as useless. Hence it is ironic that there are now whole books devoted to applications of number theory to computer science, RSA cryptography being just one such application. Furthermore, as the need for public-key cryptography has developed, techniques from other areas of mathematics, such as abstract algebra and algebraic geometry, have been used to develop additional cryptosystems.

TEST YOURSELF

1. When letters of the alphabet are encrypted using the Caesar cipher, the encrypted version of a letter is _____.
2. If a, b, and n are integers with $n > 1$, all of the following are different ways to express the fact that $n \mid (a - b)$: _____, _____, _____, _____.
3. If a, b, c, d, m, and n are integers with $n > 1$ and if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a + b \equiv$ _____, $a - b \equiv$ _____, $ab \equiv$ _____, and $a^m \equiv$ _____.
4. If a, n, and k are positive integers with $n > 1$, an efficient way to compute $a^k \pmod{n}$ is to write k as a _____ and use the facts about computing products and powers modulo n.
5. To express a greatest common divisor of two integers as a linear combination of the integers, use the extended version of the _____ algorithm.
6. To find an inverse for a positive integer a modulo an integer n with $n > 1$, you express the number 1 as _____.

7. To encrypt a message M using RSA cryptography with public key pq and e, you use the formula _____, and to decrypt a message C, you use the formula _____, where _____.

8. Euclid's lemma says that for all integers a, b, and c if $\gcd(a, c) = 1$ and $a \mid bc$, then _____.

9. Fermat's little theorem says that if p is any prime number and a is any integer such that $p \mid a$, then _____.

10. The crux of the proof that the RSA cipher works is that if (1) p and q are distinct large prime numbers, (2) $M < pq$, (3) M is relatively prime to pq, (4) e is relatively prime to $(p-1)(q-1)$, and (5) d is a positive inverse for e modulo $(p-1)(q-1)$, then $M =$ _____.

EXERCISE SET 8.4

1. **a.** Use the Caesar cipher to encrypt the message WHERE SHALL WE MEET.
   b. Use the Caesar cipher to decrypt the message LQ WKH FDIHWHULD.

2. **a.** Use the Caesar cipher to encrypt the message AN APPLE A DAY.
   b. Use the Caesar cipher to decrypt the message NHHSV WKH GRFWRU DZDB.

3. Let $a = 25$, $b = 19$, and $n = 3$.
   a. Verify that $3 \mid (25 - 19)$.
   b. Explain why $25 \equiv 19 \pmod 3$.
   c. What value of k has the property that $25 = 19 + 3k$?
   d. What is the (nonnegative) remainder obtained when 25 is divided by 3? When 19 is divided by 3?
   e. Explain why $25 \bmod 3 = 19 \bmod 3$.

4. Let $a = 68$, $b = 33$, and $n = 7$.
   a. Verify that $7 \mid (68 - 33)$.
   b. Explain why $68 \equiv 33 \pmod 7$.
   c. What value of k has the property that $68 = 33 + 7k$?
   d. What is the (nonnegative) remainder obtained when 68 is divided by 7? When 33 is divided by 7?
   e. Explain why $68 \bmod 7 = 33 \bmod 7$.

5. Prove the transitivity of modular congruence. That is, prove that for all integers a, b, c, and n with $n > 1$, if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$.

H 6. Prove that the distinct equivalence classes of the relation of congruence modulo n are the sets $[0]$, $[1]$, $[2]$, . . . , $[n-1]$, where for each $a = 0, 1, 2, \ldots, n-1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod n\}.$$

7. Verify the following statements.
   a. $128 \equiv 2 \pmod 7$ and $61 \equiv 5 \pmod 7$
   b. $(128 + 61) \equiv (2 + 5) \pmod 7$
   c. $(128 - 61) \equiv (2 - 5) \pmod 7$
   d. $(128 \cdot 61) \equiv (2 \cdot 5) \pmod 7$
   e. $128^2 \equiv 2^2 \pmod 7$

8. Verify the following statements.
   a. $45 \equiv 3 \pmod 6$ and $104 \equiv 2 \pmod 6$
   b. $(45 + 104) \equiv (3 + 2) \pmod 6$
   c. $(45 - 104) \equiv (3 - 2) \pmod 6$
   d. $(45 \cdot 104) \equiv (3 \cdot 2) \pmod 6$
   e. $45^2 \equiv 3^2 \pmod 6$

In 9–11, prove each of the given statements, assuming that a, b, c, d, and n are integers with $n > 1$ and that $a \equiv c \pmod n$ and $b \equiv d \pmod n$.

9. **a.** $(a + b) \equiv (c + d) \pmod n$
   b. $(a - b) \equiv (c - d) \pmod n$

10. $a^2 \equiv c^2 \pmod n$

11. $a^m \equiv c^m \pmod n$ for every integer $m \geq 1$ (Use mathematical induction on m.)

12. **a.** Prove that for every integer $n \geq 0$, $10^n \equiv 1 \pmod 9$.
    b. Use part (a) to prove that a positive integer is divisible by 9 if, and only if, the sum of its digits is divisible by 9.

13. **a.** Prove that for every integer $n \geq 1$, $10^n \equiv (-1)^n \pmod{11}$.
    b. Use part (a) to prove that a positive integer is divisible by 11 if, and only if, the alternating sum of its digits is divisible by 11. (For instance, the alternating sum of the digits of 82,379 is $8 - 2 + 3 - 7 + 9 = 11$ and $82{,}379 = 11 \cdot 7489$.)

14. Use the technique of Example 8.4.4 to find $14^2 \bmod 55$, $14^4 \bmod 55$, $14^8 \bmod 55$, and $14^{16} \bmod 55$.

15. Use the result of exercise 14 and the technique of Example 8.4.5 to find 14^{27} *mod* 55.

In 16–18, use the techniques of Example 8.4.4 and Example 8.4.5 to find the given numbers.

16. 675^{307} *mod* 713 **17.** 89^{307} *mod* 713

18. 48^{307} *mod* 713

In 19–24, use the RSA cipher from Examples 8.4.9 and 8.4.10. In 19–21, translate the message into its numeric equivalent and encrypt it. In 22–24, decrypt the ciphertext and translate the result into letters of the alphabet to discover the message.

19. HELLO **20.** WELCOME **21.** EXCELLENT

22. 13 20 20 09 **23.** 08 05 15 **24.** 51 14 49 15

***H* 25.** Use Theorem 5.2.2 to prove that if a and n are positive integers and $a^n - 1$ is prime, then $a = 2$ and n is prime.

In 26 and 27, use the extended Euclidean algorithm to find the greatest common divisor of the given numbers and express it as a linear combination of the two numbers.

26. 6664 and 765 **27.** 4158 and 1568

Exercises 28 and 29 refer to the following formal version of the extended Euclidean algorithm.

Algorithm 8.4.1 Extended Euclidean Algorithm
[Given integers A and B with $A > B > 0$, this algorithm computes gcd(A, B) *and finds integers s and t such that* $sA + tB =$ gcd(A, B)*.]*
Input: A, B *[integers with* $A > B > 0$*]*
Algorithm Body:
$a := A$, $b := B$, $s := 1$, $t := 0$, $u := 0$, $v := 1$,
[pre-condition: $a = sA + tB$ *and* $b = uA + vB$*]*
while $(b \neq 0)$
[loop invariant: $a = sA + tB$ *and* $b = uA + vB$, gcd$(a, b) =$ gcd(A, B)*]*
$r := a \bmod b$, $q := a \operatorname{div} b$
$a := b$, $b := r$
$newu := s - uq$, $newv := t - vq$
$s := u$, $t := v$
$u := newu$, $v := newv$
end while
gcd $:= a$
[post-condition: gcd$(A, B) = a = sA + tB$*]*
Output: gcd*[a positive integer]*, *s*, *t [integers]*

In 28 and 29, for the given values of *A* and *B*, make a table showing the value of *s*, *t*, and $sA + tB$ before the start of the *while* loop and after each iteration of the loop.

28. $A = 330$, $B = 156$ **29.** $A = 284$, $B = 168$

30. Finish the proof of Theorem 8.4.5 by proving that if a, b, and c are as in the proof, then $c \mid b$.

31. a. Find an inverse for 210 modulo 13.
b. Find a positive inverse for 210 modulo 13.
c. Find a positive solution for the congruence $210x \equiv 8 \pmod{13}$.

32. a. Find an inverse for 41 modulo 660.
b. Find the least positive solution for the following congruence: $41x \equiv 125 \pmod{660}$.

***H* 33.** Use Theorem 8.4.5 to prove that for all integers a, b, and c, if gcd$(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

34. Give a counterexample to show that the statement of exercise 33 is false if the hypothesis that gcd$(a, b) = 1$ is removed.

35. Corollary 8.4.7 guarantees the existence of an inverse modulo n for an integer a when a and n are relatively prime. Use Euclid's lemma to prove that the inverse is unique modulo n. In other words, show that if s and t are any two integers whose product with a is congruent to 1 modulo n, then s and t are congruent to each other modulo n.

In 36, 37, 39, and 40, use the RSA cipher with public key $n = 713 = 23 \cdot 31$ and $e = 43$. In 36 and 37, encode the messages into their numeric equivalents and encrypt them. In 39 and 40, decrypt the given ciphertext and find the original messages.

36. HELP **37.** COME

38. Find the least positive inverse for 43 modulo 660.

39. 675 089 089 048

40. 028 018 675 129

***H* 41. a.** Use mathematical induction and Euclid's lemma to prove that for every positive integer s, if p and $q_1, q_2, \ldots, q_s$ are prime numbers and $p \mid q_1 q_2 \cdots q_s$, then $p = q_i$ for some i with $1 \leq i \leq s$.

b. The uniqueness part of the unique factorization theorem for the integers says that given any integer n, if

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

for some positive integers r and s and prime numbers $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$ and $p_i = q_i$ for every integer i with $1 \leq i \leq r$.

Use the result of part (a) to fill in the details of the following sketch of a proof: Suppose

that n is an integer with two different prime factorizations: $n = p_1p_2 \cdots p_t = q_1q_2 \cdots q_u$. All the prime factors that appear on both sides can be cancelled (as many times as they appear on both sides) to arrive at the situation where $p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$, $p_1 \le p_2 \le \cdots \le p_r$, $q_1 \le q_2 \le \cdots \le q_s$, and $p_i \ne q_j$ for any integers i and j. Then use part (a) to deduce a contradiction, and conclude that the prime factorization of n is unique except, possibly, for the order in which the prime factors are written.

42. According to Fermat's little theorem, if p is a prime number and a and p are relatively prime, then $a^{p-1} \equiv 1 \pmod{p}$. Verify that this theorem gives correct results for the following:
a. $a = 15$ and $p = 7$ **b.** $a = 8$ and $p = 11$

43. Fermat's little theorem can be used to show that a number is not prime by finding a number a relatively prime to p with the property that $a^{p-1} \not\equiv 1 \pmod{p}$. However, it cannot be used to show that a number *is* prime. Find an example to illustrate this fact. That is, find integers a and p such that a and p are relatively prime and $a^{p-1} \equiv 1 \pmod{p}$ but p is not prime.

ANSWERS FOR TEST YOURSELF

1. the letter that is three places in the alphabet to the right of the given letter, with X wrapped around to A, Y to B, and Z to C **2.** $a \equiv b \pmod{n}$; $a = b + kn$ for some integer k; a and b have the same nonnegative remainder when divided by n; $a \bmod n = b \bmod n$ **3.** $(c + d) \pmod{n}$; $(c - d) \pmod{n}$; $(cd) \pmod{n}$; $c^m \pmod{n}$ **4.** sum of powers of 2 **5.** Euclidean **6.** a linear combination of a and n **7.** $C = M^e \bmod pq$; $M = C^d \bmod pq$; d is a positive inverse for e modulo $(p-1)(q-1)$ **8.** $a \mid b$ **9.** $a^{p-1} \equiv 1 \pmod{p}$ **10.** $M^{ed} \bmod pq$

8.5 Partial Order Relations

There is no branch of mathematics, however abstract, which may not some day be applied to phenomena of the real world. —Nicolai Ivanovitch Lobachevsky, 1792–1856

In order to obtain a degree in computer science at a certain university, a student must take a specified set of required courses, some of which must be completed before others can be started. Given the prerequisite structure of the program, one might ask what is the least number of school terms needed to fulfill the degree requirements, or what is the maximum number of courses that can be taken in the same term, or whether there is a sequence in which a part-time student can take the courses one per term. Later in this section, we will show how representing the prerequisite structure of the program as a partial order relation makes it relatively easy to answer such questions.

Antisymmetry

In Section 8.2 we defined three properties of relations: reflexivity, symmetry, and transitivity. A fourth property of relations is called *antisymmetry*. In terms of the arrow diagram of a relation, saying that a relation is antisymmetric is the same as saying that whenever there is an arrow going from one element to another *distinct* element, there is *not* an arrow going back from the second to the first.

Definition

Let R be a relation on a set A. R is **antisymmetric** if, and only if,

for every a and b in A, if $a \mathrel{R} b$ and $b \mathrel{R} a$ then $a = b$.

By taking the negation of the definition, you can see that a relation R is ***not*** **antisymmetric** if, and only if,

there are elements a and b in A such that $a \, R \, b$ and $b \, R \, a$ but $a \neq b$.

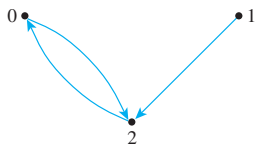
Example 8.5.1 **Testing for Antisymmetry of Finite Relations**

Let R_1 and R_2 be the relations on $\{0, 1, 2\}$ defined as follows: Draw the directed graphs for R_1 and R_2 and indicate which relations are antisymmetric.

a. $R_1 = \{(0, 2), (1, 2), (2, 0)\}$ b. $R_2 = \{(0, 0), (0, 1), (0, 2), (1, 1), (1, 2)\}$

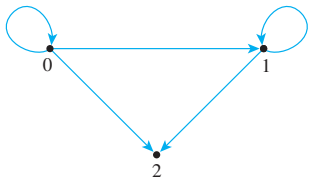
Solution

a. R_1 is not antisymmetric.



Since $0 \, R_1 \, 2$ and $2 \, R_1 \, 0$ but $0 \neq 2$, R_1 is not antisymmetric.

b. R_2 is antisymmetric.



In order for R_2 not to be antisymmetric, there would have to exist a pair of distinct elements of A such that each is related to the other by R_2. But you can see by inspection that no such pair exists.

■

Example 8.5.2 **Testing for Antisymmetry of "Divides" Relations**

Let R_1 be the "divides" relation on the set of all positive integers, and let R_2 be the "divides" relation on the set of all integers.

$$\begin{array}{lll} \text{For every } a, b \in Z^+, & a \, R_1 \, b & \Leftrightarrow \quad a \mid b. \\ \text{For every } a, b \in Z, & a \, R_2 \, b & \Leftrightarrow \quad a \mid b. \end{array}$$

a. Is R_1 antisymmetric? Prove or give a counterexample.

b. Is R_2 antisymmetric? Prove or give a counterexample.

Solution

a. R_1 is antisymmetric.

Proof: Suppose a and b are positive integers such that $a \, R_1 \, b$ and $b \, R_1 \, a$. *[We must show that $a = b$.]* By definition of R_1, $a \mid b$ and $b \mid a$. Thus, by definition of divides, there are integers k_1 and k_2 with $b = k_1 a$ and $a = k_2 b$. It follows that

$$b = k_1 a = k_1(k_2 b) = (k_1 k_2) b.$$

Dividing both sides by b gives

$$k_1 k_2 = 1.$$

Now since a and b are both integers, k_1 and k_2 are both positive integers also. And the only product of two positive integers that equals 1 is $1 \cdot 1$. Thus

$$k_1 = k_2 = 1$$

and so $$a = k_2 b = 1 \cdot b = b$$

[as was to be shown].

b. R_2 is not antisymmetric.
Counterexample:
Let $a = 2$ and $b = -2$. Then $a \mid b$ *[since* $-2 = (-1) \cdot 2$*]* and $b \mid a$ *[since* $2 = (-1)(-2)$*]*.
Hence $a \, R_2 \, b$ and $b \, R_2 \, a$ but $a \neq b$. ■

Example 8.5.2 illustrates the fact that a relation may be antisymmetric on a subset of a set but not antisymmetric on the set itself.

Partial Order Relations

A relation that is reflexive, antisymmetric, and transitive is called a *partial order.*

Definition

Let R be a relation defined on a set A. R is a **partial order relation** if, and only if, R is reflexive, antisymmetric, and transitive.

Two fundamental partial order relations are the "less than or equal to" relation on a set of real numbers and the "subset" relation on a set of sets. These can be thought of as models, or paradigms, for general partial order relations.

Example 8.5.3 **The "Subset" Relation**

Let $\mathcal{A}$ be any collection of sets and define the "subset" relation, $\subseteq$, on $\mathcal{A}$ as follows: For every $U, V \in \mathcal{A}$,

$$U \subseteq V \iff \text{for each } x, \text{ if } x \in U \text{ then } x \in V.$$

By an argument almost identical to that of the solution for exercise 23 of Section 8.2, $\subseteq$ is reflexive and transitive. Finish the proof that $\subseteq$ is a partial order relation by proving that $\subseteq$ is antisymmetric.

Solution For $\subseteq$ to be antisymmetric means that for all sets U and V in $\mathcal{A}$, if $U \subseteq V$ and $V \subseteq U$ then $U = V$. This is true by definition of equality of sets. ■

Example 8.5.4 **A "Divides" Relation on a Set of Positive Integers**

Let $\mid$ be the "divides" relation on a set A of positive integers. That is, for all a and b in A,

$$a \mid b \iff b = ka \text{ for some integer } k.$$

Prove that $\mid$ is a partial order relation on A.

Solution

| *is reflexive*: *[We must show that for each $a \in A$, $a \mid a$.]* Suppose $a \in A$. Then $a = 1 \cdot a$, so $a \mid a$ by definition of divisibility.

| *is antisymmetric*: *[We must show that for every $a, b \in A$, if $a \mid b$ and $b \mid a$ then $a = b$.]* The proof of this is virtually identical to that of Example 8.5.2(a).

| *is transitive*: To show transitivity means to show that for every $a, b, c \in A$, if $a \mid b$ and $b \mid c$ then $a \mid c$. But this is the transitivity of divisibility property, which was proved as Theorem 4.4.3.

Since | is reflexive, antisymmetric, and transitive, | is a partial order relation on A. ■

Example 8.5.5 **The "Less Than or Equal to" Relation**

Let S be a set of real numbers and define the "less than or equal to" relation, $\leq$, on S as follows: For all real numbers x and y in S,

$$x \leq y \quad \Leftrightarrow \quad x < y \text{ or } x = y.$$

Show that $\leq$ is a partial order relation.

Solution

$\leq$ *is reflexive*: For $\leq$ to be reflexive means that $x \leq x$ for every real number x in S. But $x \leq x$ means that $x < x$ or $x = x$, and $x = x$ is always true.

$\leq$ *is antisymmetric*: For $\leq$ to be antisymmetric means that for all real numbers x and y in S, if $x \leq y$ and $y \leq x$ then $x = y$. This follows immediately from the definition of $\leq$ and the trichotomy property (see Appendix A, T17), which says that given any real numbers x and y, exactly one of the following holds: $x < y$ or $x = y$ or $x > y$.

$\leq$ *is transitive*: For $\leq$ to be transitive means that for all real numbers x, y, and z in S if $x \leq y$ and $y \leq z$ then $x \leq z$. This follows from the definition of $\leq$ and the transitivity property of order (see Appendix A, T18), which says that given any real numbers x, y, and z, if $x < y$ and $y < z$ then $x < z$.

Because $\leq$ is reflexive, antisymmetric, and transitive, it is a partial order relation. ■

Notation

Because of the special paradigmatic role played by the $\leq$ relation in the study of partial order relations, the symbol $\preceq$ is often used to refer to a general partial order relation, and the notation $x \preceq y$ is read "x is less than or equal to y" or "y is greater than or equal to x."

Lexicographic Order

To figure out which of two words comes first in an English dictionary, you compare their letters one by one from left to right. If all letters have been the same to a certain point and one word runs out of letters, that word comes first in the dictionary. For example, *play* comes before *playhouse*. If all letters up to a certain point are the same and the next letters differ, then the word whose next letter is located earlier in the alphabet comes first in the dictionary. For instance, *playhouse* comes before *playmate*.

More generally, if A is any set with a partial order relation, then a *dictionary* or *lexicographic* order can be defined on a set of strings over A as indicated in the following theorem.

Theorem 8.5.1 Lexicographic Order

Let A be a set with a partial order relation R, and let S be a set of strings over A. Define a relation $\preceq$ on S as follows:

Let s and t be any strings in S of lengths m and n, respectively, where m and n are positive integers, and let s_m and t_m be the characters in the mth position for s and t, respectively.

1. If $m \leq n$ and the first m characters of s and t are the same, then $s \preceq t$.
2. If the first $m - 1$ characters in s and t are the same, $s_m \, R \, t_m$, and $s_m \neq t_m$, then $s \preceq t$.
3. If λ is the null string then $\lambda \preceq s$.

If no strings are related by $\preceq$ other than by these three conditions, then $\preceq$ is a partial order relation on S.

The proof of Theorem 8.5.1 is technical but straightforward. It is left for the exercises.

Definition

The partial order relation of Theorem 8.5.1 is called the **lexicographic order for S** that corresponds to the partial order R on A.

Example 8.5.6 **Testing Strings for Lexicographic Order**

Let $A = \{x, y\}$ and let R be the following partial order relation on A:

$$R = \{(x, x), (x, y), (y, y)\}.$$

Let S be the set of all strings over A, and denote by the lexicographic order for S that corresponds to R.

a. Is $x \preceq x$? Is $x \preceq xx$? Is $yx \preceq yxy$?

b. Is $xxxyyy \preceq xy$?

c. Is $x \preceq y$?

d. Is $\lambda \preceq xy$?

e. Is $xyy \preceq xyx$?

Solution

a. Yes in all three cases, by property (1) of the definition of $\preceq$.

b. Yes in all cases, by property (2) of the definition of $\preceq$.

c. Yes in all cases, by property (2) of the definition of $\preceq$. In this case $m - 1 = 0$, and the statement that the first zero characters of x and y are the same is true by default.

d. Yes by property (3) of the definition of $\preceq$.

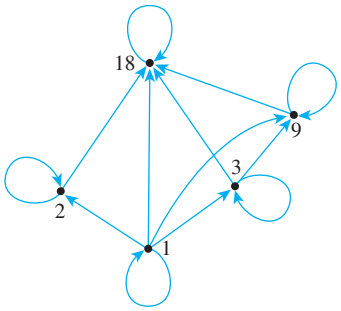
e. No because y is not related to x by R. ■

Hasse Diagrams

Let $A = \{1, 2, 3, 9, 18\}$ and consider the "divides" relation on A: For every $a, b \in A$,

$$a \mid b \iff b = ka \text{ for some integer } k.$$

The directed graph of this relation has the following appearance:

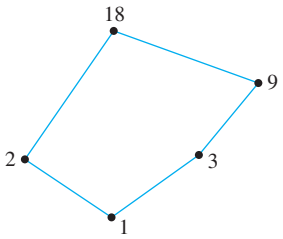


Note that there is a loop at every vertex, all other arrows point in the same direction (upward), and any time there is an arrow from one point to a second and from the second point to a third, there is an arrow from the first point to the third. Given any partial order relation defined on a finite set, it is possible to draw the directed graph in such a way that all of these properties are satisfied. This makes it possible to associate a somewhat simpler graph, called a **Hasse diagram** (after Helmut Hasse, a twentieth-century German number theorist), with a partial order relation defined on a finite set. To obtain a Hasse diagram, proceed as follows:

Start with a directed graph of the relation, placing vertices on the page so that all arrows point upward. Then eliminate

1. the loops at all the vertices,
2. all arrows whose existence is implied by the transitive property, and
3. the direction indicators on the arrows.

For the relation given previously, the Hasse diagram is as follows:



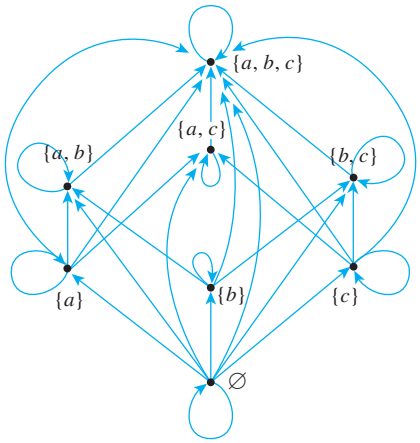
Example 8.5.7 **Constructing a Hasse Diagram**

Consider the "subset" relation, $\subseteq$, on the set $\mathcal{P}(\{a, b, c\})$. That is, for all sets U and V in $\mathcal{P}(\{a, b, c\})$,

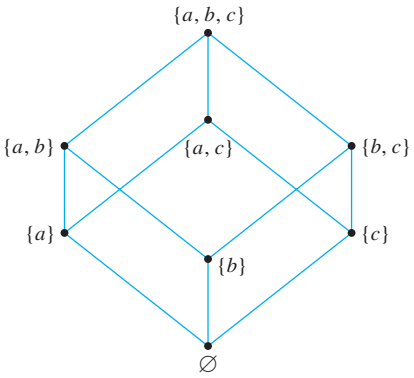
$$U \subseteq V \quad \Leftrightarrow \quad \forall x, \text{if } x \in U \text{ then } x \in V.$$

Construct the Hasse diagram for this relation.

Solution Draw the directed graph of the relation in such a way that all arrows except loops point upward.



Then strip away all loops, unnecessary arrows, and direction indicators to obtain the Hasse diagram.

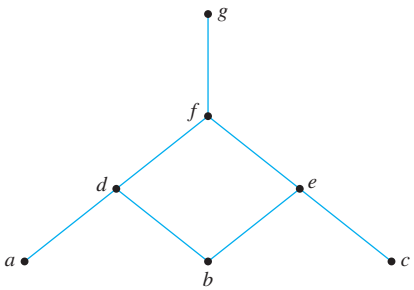


To recover the directed graph of a relation from the Hasse diagram, just reverse the instructions given previously, using the knowledge that the original directed graph was sketched so that all arrows pointed upward:

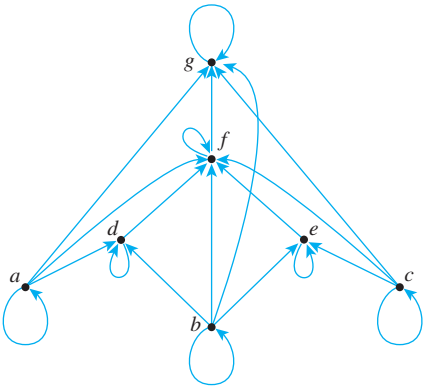
1. Reinsert the direction markers on the arrows making all arrows point upward.
2. Add loops at each vertex.
3. For each sequence of arrows from one point to a second and from that second point to a third, add an arrow from the first point to the third.

Example 8.5.8 **Obtaining the Directed Graph of a Partial Order Relation from the Hasse Diagram of the Relation**

A partial order relation R has the following Hasse diagram. Find the directed graph of R.



Solution



Partially and Totally Ordered Sets

Given any two real numbers x and y, either $x \leq y$ or $y \leq x$. In a situation like this, the elements x and y are said to be *comparable*. On the other hand, given two subsets A and B of $\{a, b, c\}$, it may be the case that neither $A \subseteq B$ nor $B \subseteq A$. For instance, let $A = \{a, b\}$ and $B = \{b, c\}$. Then $A \not\subseteq B$ and $B \not\subseteq A$. In such a case, A and B are said to be *noncomparable*.

Definition

Suppose $\preceq$ is a partial order relation on a set A. Elements a and b of A are said to be **comparable** if, and only if, either $a \preceq b$ or $b \preceq a$. Otherwise, a and b are called **noncomparable**.

When all the elements of a partial order relation are comparable, the relation is called a *total order.*

Definition

If R is a partial order relation on a set A, and for any two elements a and b in A either $a \; R \; b$ or $b \; R \; a$, then R is a **total order relation** on A.

Both the "less than or equal to" relation on sets of real numbers and the lexicographic order of the set of words in a dictionary are total order relations. Note that the Hasse diagram for a total order relation can be drawn as a single vertical "chain."

Many important partial order relations have elements that are not comparable and are, therefore, not total order relations. For instance, the subset relation on $\mathcal{P}(\{a, b, c\})$ is not a total order relation because, as shown previously, the subsets $\{a, b\}$ and $\{a, c\}$ of $\{a, b, c\}$ are not comparable. In addition, a "divides" relation is not a total order relation unless the elements are all powers of a single integer. (See exercise 21 at the end of this section.)

A set A is called a **partially ordered set** (or **poset**) with respect to a relation $\preceq$ if, and only if, $\preceq$ is a partial order relation on A. For instance, the set of real numbers is a partially ordered set with respect to the "less than or equal to" relation $\leq$, and a set of sets is partially ordered with respect to the "subset" relation $\subseteq$. It is entirely straightforward to show that *any subset of a partially ordered set is partially ordered.* (See exercise 35 at the end of this

section.) This, of course, assumes the "same definition" for the relation on the subset as for the set as a whole. A set A is called a **totally ordered set** with respect to a relation $\preceq$ if, and only if, A is partially ordered with respect to $\preceq$ and $\preceq$ is a total order.

A set that is partially ordered but not totally ordered may have totally ordered subsets. Such subsets are called *chains*.

Definition

Let A be a set that is partially ordered with respect to a relation $\preceq$. A subset B of A is called a **chain** if, and only if, the elements in each pair of elements in B are comparable. In other words, $a \preceq b$ or $b \preceq a$ for every a and b in B. The **length of a chain** is one less than the number of elements in the chain.

Observe that if B is a chain in A, then B is a totally ordered set with respect to the "restriction" of $\preceq$ to B.

Example 8.5.9 **A Chain of Subsets**

The set $\mathcal{P}(\{a, b, c\})$ is partially ordered with respect to the subset relation. Find a chain of length 3 in $\mathcal{P}(\{a, b, c\})$.

Solution Since $\varnothing \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$, the set

$$S = \{\varnothing, \{a\}, \{a, b\}, \{a, b, c\}\}$$

is a chain of length 3 in $\mathcal{P}(\{a, b, c\})$. ■

In exercise 39 at the end of this section, you are asked to show that a set that is partially ordered with respect to a relation $\preceq$ is totally ordered with respect to $\preceq$ if, and only if, it is a chain.

A *maximal element* in a partially ordered set is an element that is greater than or equal to every element *to which it is comparable*. (There may be many elements to which it is *not* comparable.) A *greatest element* in a partially ordered set is an element that is greater than or equal to *every* element in the set (so it is comparable to every element in the set). Minimal and least elements are defined similarly.

Definition

Let a set A be partially ordered with respect to a relation $\preceq$.

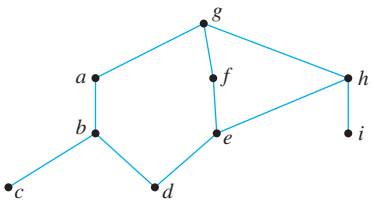
1. An element a in A is called a **maximal element of A** if, and only if, for each b in A, either $b \preceq a$ or b and a are not comparable.
2. An element a in A is called a **greatest element of A** if, and only if, for each b in A, $b \preceq a$.
3. An element a in A is called a **minimal element of A** if, and only if, for each b in A, either $a \preceq b$ or b and a are not comparable.
4. An element a in A is called a **least element of A** if, and only if, for each b in A, $a \preceq b$.

A greatest element is maximal, but a maximal element need not be a greatest element. However, every finite subset of a totally ordered set has both a least element and a greatest element. (See exercise 40 at the end of the section.) Similarly, a least element is minimal, but a minimal element need not be a least element. Furthermore, a set that is partially ordered with respect to a relation can have at most one greatest element and one least element

(see exercise 42 at the end of the section), but it may have more than one maximal or minimal element. The next example illustrates some of these facts.

Example 8.5.10 **Maximal, Minimal, Greatest, and Least Elements**

Let $A = \{a, b, c, d, e, f, g, h, i\}$ have the partial ordering $\preceq$ defined by the following Hasse diagram. Find all maximal, minimal, greatest, and least elements of A.



Solution There is just one maximal element, g, which is also the greatest element. The minimal elements are c, d, and i, and there is no least element. ■

Topological Sorting

Is it possible to input the sets of $\mathcal{P}(\{a, b, c\})$ into a computer in a way that is *compatible* with the subset relation $\subseteq$ in the sense that if set U is a subset of set V, then U is input before V? The answer, as it turns out, is yes. For instance, the following input order satisfies the given condition:

$$\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Another input order that satisfies the condition is

$$\varnothing, \{a\}, \{b\}, \{a, b\}, \{c\}, \{b, c\}, \{a, c\}, \{a, b, c\}.$$

Definition

Given partial order relations $\preceq$ and $\preceq'$ on a set A, $\preceq'$ is **compatible** with $\preceq$ if, and only if, for every a and b in A, if $a \preceq b$ then $a \preceq' b$.

Given an arbitrary partial order relation $\preceq$ on a set A, is there a total order $\preceq'$ on A that is compatible with $\preceq$? If the set on which the partial order is defined is finite, then the answer is yes. A total order that is compatible with a given order is called a *topological sorting.*

Definition

Given partial order relations $\preceq$ and $\preceq'$ on a set A, $\preceq'$ is a **topological sorting** for $\preceq$ if, and only if, $\preceq'$ is a total order that is compatible with $\preceq$.

The construction of a topological sorting for a general finite partially ordered set is based on the fact that *any partially ordered set that is finite and nonempty has a minimal element.* (See exercise 41 at the end of the section.) To create a total order for a partially ordered set, simply pick any minimal element and make it number one. Then consider the set obtained when this element is removed. Since the new set is a subset of a partially ordered set, it is partially ordered. If it is empty, stop the process. If not, pick a minimal

element from it and call that element number two. Then consider the set obtained when this element also is removed. If this set is empty, stop the process. If not, pick a minimal element and call it number three. Continue in this way until all the elements of the set have been used up.

Here is a somewhat more formal version of the algorithm:

Constructing a Topological Sorting

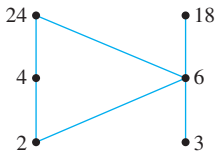
Let $\preceq$ be a partial order relation on a nonempty finite set A. To construct a topological sorting:

1. Pick any minimal element x in A. *[Such an element exists since A is nonempty.]*
2. Set $A' := A - \{x\}$.
3. Repeat steps *a–c* while $A' \neq \varnothing$.
   a. Pick any minimal element y in A'.
   b. Define $x \preceq' y$.
   c. Set $A' := A' - \{y\}$ and $x := y$.

[Completion of steps 1–3 of this algorithm gives enough information to construct the Hasse diagram for the total ordering $\preceq$. We have already shown how to use the Hasse diagram to obtain a complete directed graph for a relation.]

Example 8.5.11 **A Topological Sorting**

Consider the set $A = \{2, 3, 4, 6, 18, 24\}$ ordered by the "divides" relation $|$. The Hasse diagram of this relation is the following:

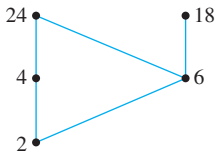


The ordinary "less than or equal to" relation $\leq$ on this set is a topological sorting for it since for positive integers a and b, if $a|b$ then $a \leq b$. Find another topological sorting for this set.

Solution The set has two minimal elements: 2 and 3. Either one may be chosen; suppose you pick 3. The beginning of the total order is

$$\text{total order: } 3.$$

Set $A' = A - \{3\}$. You can indicate this by removing 3 from the Hasse diagram as shown below.



Next choose a minimal element from $A' - \{3\}$. Only 2 is minimal, so you must pick it. The total order thus far is

$$\text{total order: } 3 \preceq 2.$$

Set $A' = (A - \{3\}) - \{2\} = A - \{3, 2\}$. You can indicate this by removing 2 from the Hasse diagram, as is shown below.

Choose a minimal element from $A' - \{3, 2\}$. Again you have two choices: 4 and 6. Suppose you pick 6. The total order for the elements chosen thus far is

$$\text{total order: } 3 \preceq 2 \preceq 6.$$

You continue in this way until every element of A has been picked. One possible sequence of choices gives

$$\text{total order: } 3 \preceq 2 \preceq 6 \preceq 18 \preceq 4 \preceq 24.$$

You can verify that this order is compatible with the "divides" partial order by checking that for each pair of elements a and b in A such that $a \mid b$, then $a \preceq b$. Note that it is *not* the case that if $a \preceq b$ then $a \mid b$. ■

An Application

To return to the example that introduced this section, note that the following defines a partial order relation on the set of courses required for a university degree: For all required courses x and y,

$$x \preceq y \quad \Leftrightarrow \quad x = y \quad \text{or} \quad x \text{ is a prerequisite for } y.$$

If the Hasse diagram for the relation is drawn, then the questions raised at the beginning of this section can be answered easily. For instance, consider the Hasse diagram for the requirements at a particular university, which is shown in Figure 8.5.1.

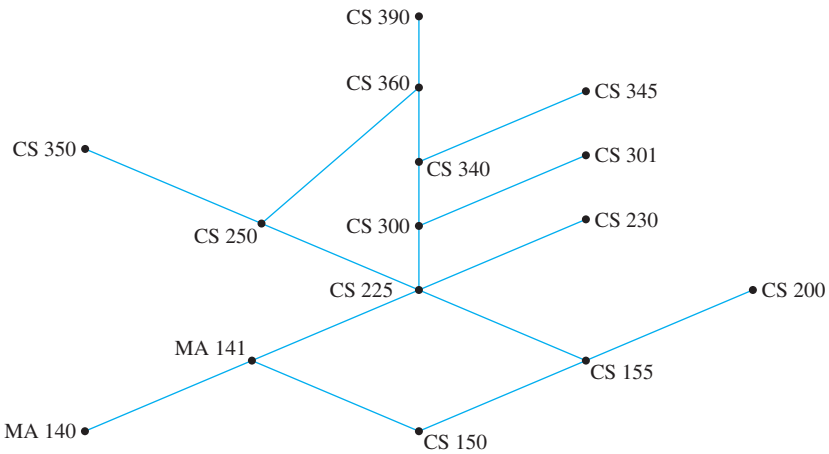


FIGURE 8.5.1

The minimum number of school terms needed to complete the requirements is the size of a longest chain, which is 7 (150, 155, 225, 300, 340, 360, 390, for example). The maximum number of courses that could be taken in the same term (assuming the university allows it) is the maximum number of noncomparable courses, which is 6 (350, 360, 345, 301, 230, 200, for example). A part-time student could take the courses in a sequence

determined by constructing a topological sorting for the set. (One such sorting is 140, 150, 141, 155, 200, 225, 230, 300, 250, 301, 340, 345, 350, 360, 390. There are many others.)

PERT and CPM

Two important and widely used applications of partial order relations are **PERT** (Program Evaluation and Review Technique) and **CPM** (Critical Path Method). These techniques were developed in the 1950s as planners came to grips with the complexities of scheduling the individual activities needed to complete very large projects, and although they are very similar, their developments were independent. PERT was developed by the U.S. Navy to help organize the construction of the Polaris submarine, and CPM was developed by the E. I. Du Pont de Nemours company for scheduling chemical plant maintenance. Here is a somewhat simplified example of the way the techniques work.

Example 8.5.12 **A Job Scheduling Problem**

At an automobile assembly plant, the job of assembling an automobile can be broken down into these tasks:

1. Build frame.
2. Install engine, power train components, gas tank.
3. Install brakes, wheels, tires.
4. Install dashboard, floor, seats.
5. Install electrical lines.
6. Install gas lines.
7. Install brake lines.
8. Attach body panels to frame.
9. Paint body.

Certain of these tasks can be carried out at the same time, whereas some cannot be started until other tasks are finished. Table 8.5.1 summarizes the order in which tasks can be performed and the time required to perform each task.

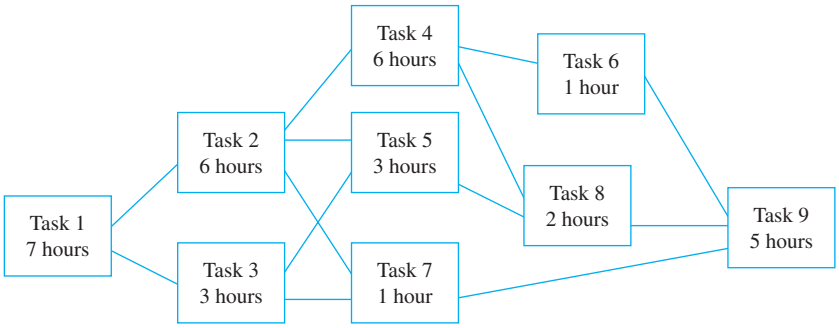
TABLE 8.5.1

Task	Immediately Preceding Tasks	Time Needed to Perform Task
1		7 hours
2	1	6 hours
3	1	3 hours
4	2	6 hours
5	2, 3	3 hours
6	4	1 hour
7	2, 3	1 hour
8	4, 5	2 hours
9	6, 7, 8	5 hours

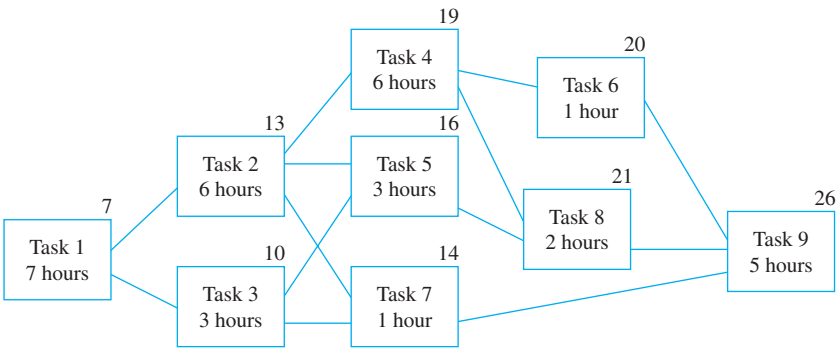
Let T be the set of all tasks, and consider the partial order relation $\preceq$ defined on T as follows: For all tasks x and y in T,

$$x \preceq y \quad \Leftrightarrow \quad x = y \text{ or } x \text{ precedes } y.$$

If the Hasse diagram of this relation is turned sideways (as is customary in PERT and CPM analysis), it has the appearance shown below.



What is the minimum time required to assemble a car? You can determine this by working from left to right across the diagram, noting for each task (say, just above the box representing that task) the minimum time needed to complete that task starting from the beginning of the assembly process. For instance, you can put a 7 above the box for task 1 because task 1 requires 7 hours. Task 2 requires completion of task 1 (7 hours) plus 6 hours for itself, so the minimum time required to complete task 2, starting at the beginning of the assembly process, is $7 + 6 = 13$ hours. So you can put a 13 above the box for task 2. Similarly, you can put a 10 above the box for task 3 because $7 + 3 = 10$. Now consider what number you should write above the box for task 5. The minimum times to complete tasks 2 and 3, starting from the beginning of the assembly process, are 13 and 10 hours respectively. Since *both* tasks must be completed before task 5 can be started, the minimum time to complete task 5, starting from the beginning, is the time needed for task 5 itself (3 hours) plus the *maximum* of the times to complete tasks 2 and 3 (13 hours), and this equals $3 + 13 = 16$ hours. Thus you should place the number 16 above the box for task 5. The same reasoning leads you to place a 14 above the box for task 7. Similarly, you can place a 19 above the box for task 4, a 20 above the box for task 6, a 21 above the box for task 8, and a 26 above the box for task 9, as shown below.



This analysis shows that at least 26 hours are required to complete task 9 starting from the beginning of the assembly process. When task 9 is finished, the assembly is complete, so 26 hours is the minimum time needed to accomplish the whole process.

Note that the minimum time required to complete tasks 1, 2, 4, 8, and 9 in sequence is exactly 26 hours. This means that a delay in performing any one of these tasks causes a delay in the total time required for assembly of the car. For this reason, the path through tasks 1, 2, 4, 8, and 9 is called a **critical path**. ■

TEST YOURSELF

1. For a relation R on a set A to be antisymmetric means that _____.
2. To show that a relation R on an infinite set A is antisymmetric, you suppose that _____ and you show that _____.
3. To show that a relation R on a set A is not antisymmetric, you _____.
4. To construct a Hasse diagram for a partial order relation, you start with a directed graph of the relation in which all arrows point upward and you eliminate _____, _____, and _____.
5. If A is a set that is partially ordered with respect to a relation $\preceq$ and if a and b are elements of A, we say that a and b are comparable if, and only if, _____ or _____.
6. A relation $\preceq$ on a set A is a total order if, and only if, _____.
7. If A is a set that is partially ordered with respect to a relation $\preceq$, and if B is a subset of A, then B is a chain if, and only if, for all a and b in B, _____.
8. Let A be a set that is partially ordered with respect to a relation $\preceq$, and let a be an element of A.
   (a) a is maximal if, and only if, _____.
   (b) a is a greatest element of A if, and only if, _____.
   (c) a is minimal if, and only if, _____.
   (d) a is a least element of A if, and only if, _____.
9. Given a set A that is partially ordered with respect to a relation $\preceq$, the relation $\preceq'$ is a topological sorting for $\preceq$, if, and only if, $\preceq'$ is a _____ and for all a and b in A if $a \preceq b$ then _____.
10. PERT and CPM are used to produce efficient _____.

EXERCISE SET 8.5

1. Each of the following is a relation on $\{0, 1, 2, 3\}$. Draw directed graphs for each relation, and indicate which relations are antisymmetric.
   a. $R_1 = \{(0, 0), (0, 2), (1, 0), (1, 3), (2, 2), (3, 0), (3, 1)\}$
   b. $R_2 = \{(0, 1), (0, 2), (1, 1), (1, 2), (1, 3), (2, 2), (3, 2)\}$
   c. $R_3 = \{(0, 0), (0, 3), (1, 0), (1, 3), (2, 2), (3, 3), (3, 2)\}$
   d. $R_4 = \{(0, 0), (1, 0), (1, 2), (1, 3), (2, 0), (2, 1), (3, 2), (3, 0)\}$
2. Let P be the set of all people in the world and define a relation R on P as follows: For all people x and y,

   $$x \, R \, y \iff x \text{ is no older than } y.$$

   Is R antisymmetric? Prove or give a counterexample.
3. Let S be the set of all strings of a's and b's. Define a relation R on S as follows: For every $s, t \in S$,

   $$s \, R \, t \iff L(s) \leq L(t),$$

   where $L(x)$ denotes the length of a string x. Is R antisymmetric? Prove or give a counterexample.
4. Let R be the "less than" relation on $\mathbf{R}$, the set of all real numbers: For every $x, y \in \mathbf{R}$,

   $$x \, R \, y \iff x < y.$$

   Is R antisymmetric? Prove or give a counterexample.
5. Let $\mathbf{R}$ be the set of all real numbers and define a relation R on $\mathbf{R} \times \mathbf{R}$ as follows: For every (a, b) and (c, d) in $\mathbf{R} \times \mathbf{R}$,

   $$(a, b) \, R \, (c, d) \iff \text{either } a < c \text{ or both } a = c \text{ and } b \leq d.$$

   Is R a partial order relation? Prove or give a counterexample.
6. Let P be the set of all people who have ever lived and define a relation R on P as follows: For every $r, s \in P$,

   $$r \, R \, s \iff r \text{ is an ancestor of } s \text{ or } r = s.$$

   Is R a partial order relation? Prove or give a counterexample.

7. Define a relation R on $\mathbf{Z}$, the set of all integers as follows: For every $m, n \in \mathbf{Z}$,

$$m \, R \, n \quad \Leftrightarrow \quad \text{every prime factor of } m \text{ is a prime factor of } n.$$

Is R a partial order relation? Prove or give a counterexample.

8. Define a relation R on $\mathbf{Z}$, the set of all integers as follows: For every $m, n \in \mathbf{Z}$,

$$m \, R \, n \quad \Leftrightarrow \quad m + n \text{ is even.}$$

Is R a partial order relation? Prove or give a counterexample.

9. Define a relation R on $\mathbf{R}$, the set of all real numbers as follows: For every $x, y \in \mathbf{R}$,

$$x \, R \, y \quad \Leftrightarrow \quad x^2 \leq y^2.$$

Is R a partial order relation? Prove or give a counterexample.

10. Suppose R and S are antisymmetric relations on a set A. Must $R \cup S$ also be antisymmetric? Explain.

11. Let $A = \{a, b\}$, and suppose A has the partial order relation R where $R = \{(a, a), (a, b), (b, b)\}$. Let S be the set of all strings in a's and b's and let be the corresponding lexicographic order on S. Indicate which of the following statements are true, and for each true statement cite as a reason part (1), (2), or (3) of the definition of lexicographic order given in Theorem 8.5.1.

a. $aab \preceq aaba$ **b.** $bbab \preceq bba$
c. $\lambda \preceq aba$ **d.** $aba \preceq abb$
e. $bbab \preceq bbaa$ **f.** $ababa \preceq ababaa$
g. $bbaba \preceq bbabb$

12. Prove Theorem 8.5.1.

13. Let $A = \{a, b\}$. Describe all partial order relations on A.

14. Let $A = \{a, b, c\}$.

a. Describe all partial order relations on A for which a is a maximal element.
b. Describe all partial order relations on A for which a is a minimal element.

***H* 15.** Suppose a relation R on a set A is reflexive, symmetric, transitive, and antisymmetric. What can you conclude about R? Prove your answer.

16. Consider the "divides" relation on each of the following sets A. Draw the Hasse diagram for each relation.

a. $A = \{1, 2, 4, 5, 10, 15, 20\}$
b. $A = \{2, 3, 4, 6, 8, 9, 12, 18\}$

17. Consider the "subset" relation on $\mathcal{P}(S)$ for each of the following sets S. Draw the Hasse diagram for each relation.

a. $S = \{0, 1\}$ **b.** $S = \{0, 1, 2\}$

18. Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S$ as follows: For all ordered pairs (a, b) and (c, d) in $S \times S$,

$$(a, b) \, R \, (c, d) \quad \Leftrightarrow \quad \text{either } a < c \text{ or both } a = c \text{ and } b \leq d,$$

where $<$ denotes the usual "less than" and $\leq$ denotes the usual "less than or equal to" relation for real numbers. Draw the Hasse diagram for R.

19. Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S$ as follows: For all ordered pairs (a, b) and (c, d) in $S \times S$,

$$(a, b) \, R \, (c, d) \quad \Leftrightarrow \quad a \leq c \text{ and } b \leq d,$$

where $\leq$ denotes the usual "less than or equal to" relation for real numbers. Draw the Hasse diagram for R.

20. Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S \times S$ as follows: For all ordered triples (a, b, c) and (d, e, f) in $S \times S \times S$,

$$(a, b, c) \; R \; (d, e, f) \quad \Leftrightarrow \quad a \leq d, b \leq e, \text{ and } c \leq f,$$

where $\leq$ denotes the usual "less than or equal to" relation for real numbers. Draw the Hasse diagram for R.

21. Consider the "divides" relation defined on the set $A = \{1, 2, 2^2, 2^3, \ldots, 2^n\}$, where n is a nonnegative integer.

a. Prove that this relation is a total order relation on A.
b. Draw the Hasse diagram for this relation for $n = 4$.

In 22–29, find all greatest, least, maximal, and minimal elements for the relations in each of the referenced exercises.

22. Exercise 16(a) **23.** Exercise 16(b)
24. Exercise 17(a) **25.** Exercise 17(b)
26. Exercise 18 **27.** Exercise 19
28. Exercise 20 **29.** Exercise 21

30. Each of the following sets is partially ordered with respect to the "less than or equal to" relation, $\leq$, for real numbers. In each case, determine whether the set has a greatest or least element.

a. $\mathbf{R}$ **b.** $\{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$

c. $\{x \in \mathbf{R} \mid 0 < x < 1\}$ **d.** $\{x \in \mathbf{Z} \mid 0 < x < 10\}$

31. Let $A = \{a, b, c, d\}$, and let R be the relation

$$R = \{(a, a), (b, b), (c, c), (d, d), (c, a), (a, d), (c, d), (b, c), (b, d), (b, a)\}.$$

Is R a total order on A? Justify your answer.

32. Let $A = \{a, b, c, d\}$, and let R be the relation

$$R = \{(a, a), (b, b), (c, c), (d, d), (c, b), (a, d), (b, a), (b, d), (c, d), (c, a)\}.$$

Is R a total order on A? Justify your answer.

33. Consider the set $A = \{12, 24, 48, 3, 9\}$ ordered by the "divides" relation. Is A totally ordered with respect to the relation? Justify your answer.

***H* 34.** Suppose that R is a partial order relation on a set A and that B is a subset of A. The **restriction of R to B** is defined as follows:

$$\text{The restriction of } R \text{ to } B = \{(x, y) \mid x \in B, y \in B, \text{ and } (x, y) \in R\}.$$

In other words, two elements of B are related by the restriction of R to B if, and only if, they are related by R. Prove that the restriction of R to B is a partial order relation on B. (In less formal language, this says that a subset of a partially ordered set is partially ordered.)

35. The set $\mathcal{P}(\{w, x, y, z\})$ is partially ordered with respect to the "subset" relation $\subseteq$. Find a chain of length 4 in $\mathcal{P}(\{w, x, y, z\})$.

36. The set $A = \{2, 4, 3, 6, 12, 18, 24\}$ is partially ordered with respect to the "divides" relation. Find a chain of length 3 in A.

37. Find a chain of length 2 for the relation defined in exercise 19.

38. Prove that a partially ordered set is totally ordered if, and only if, it is a chain.

39. Suppose that A is a totally ordered set. Use mathematical induction to prove that for any integer $n \geq 1$, every subset of A with n elements has both a least element and a greatest element.

40. Prove that a nonempty, finite, partially ordered set has

a. at least one minimal element,

b. at least one maximal element.

41. Prove that a finite, partially ordered set has

a. at most one greatest element,

b. at most one least element.

42. Draw a Hasse diagram for a partially ordered set that has two maximal elements and two minimal elements and is such that each element is comparable to exactly two other elements.

43. Draw a Hasse diagram for a partially ordered set that has three maximal elements and three minimal elements and is such that each element is either greater than or less than exactly two other elements.

44. Use the algorithm given in the text to find a topological sorting for the relation of exercise 16(a) that is different from the "less than or equal to" relation $\leq$.

45. Use the algorithm given in the text to find a topological sorting for the relation of exercise 16(b) that is different from the "less than or equal to" relation $\leq$.

46. Use the algorithm given in the text to find a topological sorting for the relation of exercise 19.

47. Use the algorithm given in the text to find a topological sorting for the relation of exercise 20.

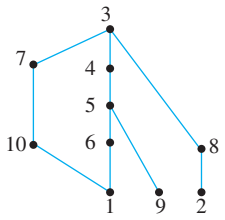
48. Use the algorithm given in the text to find a topological sorting for the "subset" relation on $\mathcal{P}(\{a, b, c, d\})$.

49. Refer to the prerequisite structure shown in Figure 8.5.1.

a. Find a list of six noncomparable courses that is different from the list given in the text.

b. Find two topological sortings that are different from the one given in the text.

50. A set S of jobs can be ordered by writing $x \preceq y$ to mean that either $x = y$ or x must be done before y, for all x and y in S. The following is a Hasse diagram for this relation for a particular set S of jobs.



a. If one person is to perform all the jobs, one after another, find an order in which the jobs can be done.

b. Suppose enough people are available to perform any number of jobs simultaneously.

(i) If each job requires one day to perform, what is the least number of days needed to perform all ten jobs?

(ii) What is the maximum number of jobs that can be performed at the same time?

51. Suppose the tasks described in Example 8.5.12 require the following performance times:

Task	Time Needed to Perform Task
1	9 hours
2	7 hours
3	4 hours
4	5 hours
5	7 hours
6	3 hours
7	2 hours
8	4 hours
9	6 hours

a. What is the minimum time required to assemble a car?

b. Find a critical path for the assembly process.

ANSWERS FOR TEST YOURSELF

1. for every a and b in A, if $a \; R \; b$ and $b \; R \; a$ then $a = b$ **2.** a and b are any elements of A with $a \; R \; b$ and $b \; R \; a$; $a = b$ **3.** show that there are elements a and b in A such that $a \; R \; b$ and $b \; R \; a$ and $a \neq b$ **4.** all loops; all arrows whose existence is implied by the transitive property; the direction indicators on the arrows **5.** $a \preceq b$; $b \preceq a$ **6.** for any two elements a and b in A, either $a \preceq b$ or $b \preceq a$ **7.** a and b are comparable **8.** (a) for every b in A either $b \preceq a$ or b and a are not comparable (b) for every b in A, $b \preceq a$ (c) for every b in A either $a \preceq b$ or b and a are not comparable (d) for every b in A, $a \preceq b$ **9.** total order; $a \prec' b$ **10.** scheduling of tasks

CHAPTER 9 COUNTING AND PROBABILITY

"It's as easy as 1–2–3."

That's the saying. And in certain ways, counting *is* easy. But other aspects of counting aren't so simple. Have you ever agreed to meet a friend "in three days" and then realized that you and your friend might mean different things? For example, on the European continent, to meet in eight days means to meet on the same day as today one week hence; on the other hand, in English-speaking countries, to meet in seven days means to meet one week hence. The difference is that on the continent, all days including the first and the last are counted. In the English-speaking world, it's the number of 24-hour periods that are counted.

Continental countries	1 ↕ Sun	2 ↕ Mon	3 ↕ Tue	4 ↕ Wed	5 ↕ Thu	6 ↕ Fri	7 ↕ Sat	8 ↕ Sun
English-speaking countries	1	2	3	4	5	6	7	

The English convention for counting days follows the almost universal convention for counting hours. If it is 9 A.M. and two people anywhere in the world agree to meet in three hours, they mean that they will get back together again at 12 noon.

Musical intervals, on the other hand, are universally reckoned the way the Continentals count the days of a week. An interval of a third consists of two tones with a single tone in between, and an interval of a second consists of two adjacent tones. (See Figure 9.1.1.)

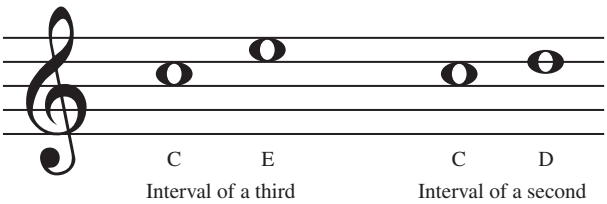


FIGURE 9.1.1

Of course, the complicating factor in all these examples is not how to count but rather what to count. And, indeed, in the more complex mathematical counting problems discussed in this chapter, it is what to count that is the central issue.

9.1 Introduction to Probability

Imagine tossing two coins and observing whether 0, 1, or 2 heads are obtained. It would be natural to guess that each of these events occurs about one-third of the time, but in fact this is not the case. Table 9.1.1 shows actual data obtained from tossing two quarters 50 times.

TABLE 9.1.1 Experimental Data Obtained from Tossing Two Quarters 50 Times

Event	Tally	Frequency (Number of times the event occurred)	Relative Frequency (Fraction of times the event occurred)
2 heads obtained	𝍸 𝍸 |	11	22%
1 head obtained	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 ||	27	54%
0 heads obtained	𝍸 𝍸 ||	12	24%

As you can see, the relative frequency of obtaining exactly 1 head was roughly twice as great as that of obtaining either 2 heads or 0 heads. It turns out that the mathematical theory of probability can be used to predict that a result like this will almost always occur. To see how, call the two coins A and B, and suppose that each is perfectly balanced. Then each has an equal chance of coming up heads or tails, and when the two are tossed together, the four outcomes pictured in Figure 9.1.2 are all equally likely.

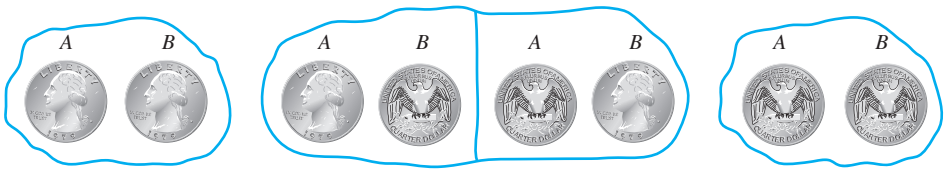


FIGURE 9.1.2 Equally Likely Outcomes from Tossing Two Balanced Coins

Figure 9.1.2 shows that there is a 1 in 4 chance of obtaining two heads and a 1 in 4 chance of obtaining no heads. The chance of obtaining one head, however, is 2 in 4 because either A could come up heads and B tails or B could come up heads and A tails. So if you repeatedly toss two balanced coins and record the number of heads, you should expect relative frequencies similar to those shown in Table 9.1.1.

To formalize this analysis and extend it to more complex situations, we introduce the notions of random process, sample space, event, and probability. To say that a process is **random** means that when it takes place, one outcome from some set of outcomes is sure to occur, but it is impossible to predict with certainty which outcome that will be. For instance, if an ordinary person performs the experiment of tossing an ordinary coin into the air and allowing it to fall flat on the ground, it can be predicted with certainty that the coin will land either heads up or tails up (so the set of outcomes can be denoted {heads, tails}), but it is not known for sure whether heads or tails will occur. We restricted this experiment to ordinary people because a skilled magician can toss a coin in a way that appears random but is not, and a physicist equipped with first-rate measuring devices may be able to analyze all the forces on the coin and correctly predict its landing position. Just a few of many examples of random processes or experiments are choosing winners in state lotteries, selecting respondents in public opinion polls, and choosing subjects to receive treatments or serve as controls in medical experiments. The set of outcomes that can result from a random process or experiment is called a *sample space*.

Definition

A **sample space** is the set of all possible outcomes of a random process or experiment. An **event** is a subset of a sample space.

In the case where an experiment has finitely many outcomes and all outcomes are equally likely to occur, the *probability* of an event (set of outcomes) is just the ratio of the number of outcomes in the event to the total number of outcomes. Strictly speaking, this result can be deduced from a set of axioms for probability formulated in 1933 by the Russian mathematician A. N. Kolmogorov. In Section 9.8 we discuss the axioms and show how to derive their consequences formally. At present, we take a less formal approach to probability and simply state the result as a principle.

Equally Likely Probability Formula

If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability of E**, denoted $P(E)$, is

$$P(E) = \frac{\text{the number of outcomes in } E}{\text{the total number of outcomes in } S}.$$

Notation

For any finite set A, $N(A)$ denotes the number of elements in A.

With this notation, the equally likely probability formula becomes

$$P(E) = \frac{N(E)}{N(S)}.$$

Example 9.1.1 **Probabilities for a Deck of Cards**

An ordinary deck of cards contains 52 cards divided into four *suits*. The *red suits* are diamonds (♦) and hearts (♥), and the *black suits* are clubs (♣) and spades (♠). Each suit contains 13 cards of the following *denominations:* 2, 3, 4, 5, 6, 7, 8, 9, 10, J (jack), Q (queen), K (king), and A (ace). The cards J, Q, and K are called *face cards.*

Mathematician Persi Diaconis, working with David Aldous in 1986 and Dave Bayer in 1992, showed that seven shuffles are needed to "thoroughly mix up" the cards in an ordinary deck. In 2000 mathematician Nick Trefethen, working with his father, Lloyd Trefethen, a mechanical engineer, used a somewhat different definition of "thoroughly mix up" to show that six shuffles will nearly always suffice. Imagine that the cards in a deck have become—by some method—so thoroughly mixed up that if you spread them out face down and pick one at random, you are as likely to get any one card as any other.

a. What is the sample space of outcomes?

b. What is the event that the chosen card is a black face card?

c. What is the probability that the chosen card is a black face card?

Solution

a. The outcomes in the sample space S are the 52 cards in the deck.

b. Let E be the event that a black face card is chosen. The outcomes in E are the jack, queen, and king of clubs and the jack, queen, and king of spades. Symbolically:

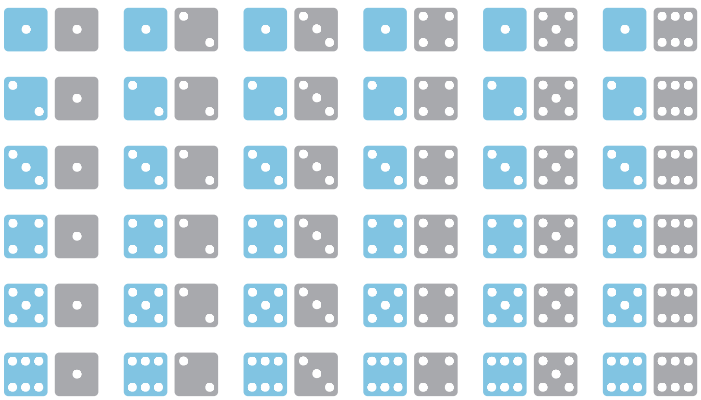
$$E = \{J\clubsuit, Q\clubsuit, K\clubsuit, J\spadesuit, Q\spadesuit, K\spadesuit\}.$$

c. By part (b), $N(E) = 6$, and according to the description of the situation, all 52 outcomes in the sample space are equally likely. Therefore, by the equally likely probability formula, the probability that the chosen card is a black face card is

$$P(E) = \frac{N(E)}{N(S)} = \frac{6}{52} \cong 11.5\%$$ ■

Example 9.1.2 **Rolling a Pair of Dice**

A die is one of a pair of dice. It is a cube with six sides, each containing from one to six dots, called *pips*. Suppose a blue die and a gray die are rolled together, and the numbers of dots that occur face up on each are recorded. The possible outcomes can be listed as follows, where in each case the die on the left is blue and the one on the right is gray.



A more compact notation identifies, say,  with the notation 24,  with 53, and so forth.

a. Use the compact notation to write the sample space S of possible outcomes.

b. Use set notation to write the event E that the numbers showing face up have a sum of 6 and find the probability of this event.

Solution

a. $S = \{11, 12, 13, 14, 15, 16, 21, 22, 23, 24, 25, 26, 31, 32, 33, 34, 35, 36, 41, 42, 43, 44, 45, 46, 51, 52, 53, 54, 55, 56, 61, 62, 63, 64, 65, 66\}$.

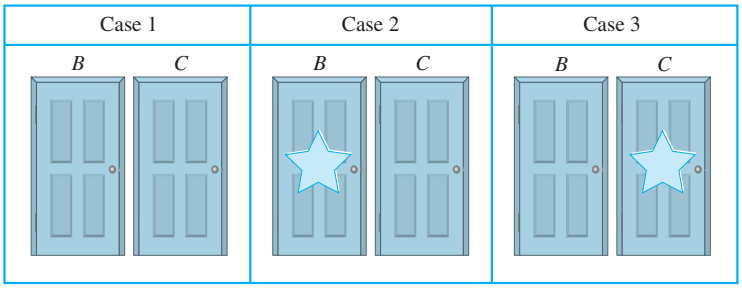
b. $E = \{15, 24, 33, 42, 51\}$.

The probability that the sum of the numbers is 6 $= P(E) = \dfrac{N(E)}{N(S)} = \dfrac{5}{36}$. ■

The next example is called the Monty Hall problem, named for the first host of the game show "Let's Make A Deal." When it was originally publicized in a newspaper column and on a radio show, it created tremendous controversy. Many highly educated people, even some with Ph.D.'s, submitted incorrect solutions or argued vociferously against the correct solution. Before you read the answer, think about what your own response to the situation would be.

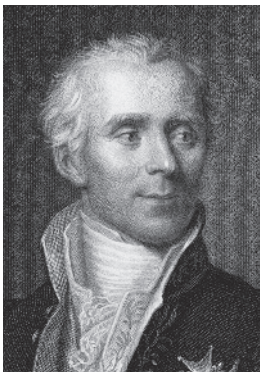
Example 9.1.3 **The Monty Hall Problem**

There are three doors on the set for a game show. Let's call them *A*, *B*, and *C*. If you pick the correct door, you win the prize. You pick door *A*. The host of the show then opens one of the other doors and reveals that there is no prize behind it. Keeping the remaining two doors closed, he asks you whether you want to switch your choice to the other closed door or stay with your original choice of door *A*. What should you do if you want to maximize your chance of winning the prize: stay with door *A* or switch—or would the likelihood of winning be the same either way?



Solution At the point just before the host opens one of the closed doors, there is no information about the location of the prize. Thus there are three equally likely possibilities for what lies behind the doors: (Case 1) the prize is behind *A* (meaning it is not behind either *B* or *C*); (Case 2) the prize is behind *B*; or (Case 3) the prize is behind *C*.

Since there is no prize behind the door the host opens, in Case 1 the host could open either door and you would win by staying with your original choice: door A. In Case 2 the host must open door *C*, and so you would win by switching to door B. In Case 3 the host must open door *B*, and so you would win by switching to door *C*. Thus, in two of the three equally likely cases, you would win by switching from *A* to the other closed door. In only one of the three equally likely cases would you win by staying with your original choice. Therefore, you should switch. ■



Bettmann/Getty Images

Pierre-Simon Laplace (1749–1827)

The analysis used for the solution in Example 9.1.3 applies only if the host *always* opens one of the closed doors and offers the contestant the choice of staying with the original choice or switching. In the original show, the host made this offer only occasionally—most often when he knew the contestant had already chosen the correct door.

Many of the fundamental principles of probability were formulated in the mid-1600s in an exchange of letters between Pierre de Fermat and Blaise Pascal in response to questions posed by a French nobleman interested in games of chance. In 1812, Pierre-Simon Laplace published the first general mathematical treatise on the subject and extended the range of applications to a variety of scientific and practical problems.

Counting the Elements of a List

Some counting problems are as simple as counting the elements of a list. For instance, how many integers are there from 5 through 12? To answer this question, imagine going along the list of integers from 5 to 12, counting each in turn.

list:	5	6	7	8	9	10	11	12
	↕	↕	↕	↕	↕	↕	↕	↕
count:	1	2	3	4	5	6	7	8

So the answer is 8.

More generally, if m and n are integers and $m \le n$, how many integers are there from m through n? To answer this question, note that $n = m + (n - m)$, where $n - m \ge 0$ *[since $n \ge m$]*. Note also that the element $m + 0$ is the first element of the list, the element $m + 1$ is the second element, the element $m + 2$ is the third, and so forth. In general, the element $m + i$ is the $(i + 1)$st element of the list.

list:	$m\ (=m+0)$	$m+1$	$m+2$	...	$n\ (=m+(n-m))$
	↕	↕	↕		↕
count:	1	2	3	...	$(n-m)+1$

And so the number of elements in the list is $n - m + 1$.

This general result is important enough to be restated as a theorem, the formal proof of which uses mathematical induction. (See exercise 33 at the end of this section.) The heart of the proof is the observation that if the list $m, m + 1, \ldots, k$ has $k - m + 1$ numbers, then the list $m, m + 1, \ldots, k, k + 1$ has $(k - m + 1) + 1 = (k + 1) - m + 1$ numbers.

Theorem 9.1.1 The Number of Elements in a List

If m and n are integers and $m \le n$, then there are $n - m + 1$ integers from m to n inclusive.

Example 9.1.4 **Counting the Elements of a Sublist**

a. How many three-digit integers (integers from 100 to 999 inclusive) are divisible by 5?

b. What is the probability that a randomly chosen three-digit integer is divisible by 5?

Solution

a. Imagine writing the three-digit integers in a row, noting those that are multiples of 5 and drawing arrows between each such integer and its corresponding multiple of 5.

100	101	102	103	104	105	106	107	108	109	110	...	994	995	996	997	998	999
↕					↕					↕			↕				
$5 \cdot 20$					$5 \cdot 21$					$5 \cdot 22$			$5 \cdot 199$				

From the sketch it is clear that there are as many three-digit integers that are multiples of 5 as there are integers from 20 to 199 inclusive. By Theorem 9.1.1, there are $199 - 20 + 1$, or 180, such integers. Hence there are 180 three-digit integers that are divisible by 5.

b. By Theorem 9.1.1 the total number of integers from 100 through 999 is $999 - 100 + 1 = 900$. By part (a), 180 of these are divisible by 5. Hence the probability that a randomly chosen three-digit integer is divisible by 5 is $180/900 = 1/5$. ■

Example 9.1.5 **Application: Counting Elements of a One-Dimensional Array**

Analysis of many computer algorithms requires skill at counting the elements of a one-dimensional array. Let $A[1], A[2], \ldots, A[n]$ be a one-dimensional array, where n is a positive integer.

a. Suppose the array is cut at a middle value $A[m]$ so that two subarrays are formed:

$$(1)\ A[1], A[2], \ldots, A[m] \quad \text{and} \quad (2)\ A[m+1], A[m+2], \ldots, A[n].$$

How many elements does each subarray have?

b. What is the probability that a randomly chosen element of the array has an even subscript

(i) if n is even? (ii) if n is odd?

Solution

a. Array (1) has the same number of elements as the list of integers from 1 through m. So by Theorem 9.1.1, it has m, or $m - 1 + 1$, elements. Array (2) has the same number of elements as the list of integers from $m + 1$ through n. So by Theorem 9.1.1, it has $n - m$, or $n - (m + 1) + 1$, elements.

b. (i) If n is even, each even subscript starting with 2 and ending with n can be matched up with an integer from 1 to $n/2$.

1	2	3	4	5	6	7	8	9	10	...	n
	↕		↕		↕		↕		↕		↕
	$2\cdot1$		$2\cdot2$		$2\cdot3$		$2\cdot4$		$2\cdot5$		$2\cdot(n/2)$

So there are $n/2$ array elements with even subscripts. Since the entire array has n elements, the probability that a randomly chosen element has an even subscript is

$$\frac{n/2}{n} = \frac{1}{2}.$$

(ii) If n is odd, then the greatest even subscript of the array is $n - 1$. So there are as many even subscripts between 1 and n as there are from 2 through $n - 1$. Then the reasoning of (i) can be used to conclude that there are $(n - 1)/2$ array elements with even subscripts.

1	2	3	4	5	6	...	$n-1$	n
	↕		↕		↕		↕	
	$2\cdot1$		$2\cdot2$		$2\cdot3$	...	$2\cdot[(n-1)/2)]$	

Since the entire array has n elements, the probability that a randomly chosen element has an even subscript is

$$\frac{(n-1)/2}{n} = \frac{n-1}{2n}.$$

Observe that as n gets larger and larger, this probability gets closer and closer to $1/2$.

Note that the answers to (i) and (ii) can be combined using the floor notation. By Theorem 4.6.2, the number of array elements with even subscripts is $\lfloor n/2 \rfloor$, so the probability that a randomly chosen element has an even subscript is $\dfrac{\lfloor n/2 \rfloor}{n}$. ■

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. A sample space of a random process or experiment is _____.
2. An event in a sample space is _____.
3. To compute the probability of an event using the equally likely probability formula, you take the ratio of the _____ to the _____.
4. If $m \leq n$, the number of integers from m to n inclusive is _____.

EXERCISE SET 9.1*

1. Toss two coins 30 times and make a table showing the relative frequencies of 0, 1, and 2 heads. How do your values compare with those shown in Table 9.1.1?

2. In the example of tossing two quarters, what is the probability that at least one head is obtained? that coin A is a head? that coins A and B are either both heads or both tails?

In 3–6 use the sample space given in Example 9.1.1. Write each event as a set and compute its probability.

3. The event that the chosen card is red and is not a face card.

4. The event that the chosen card is black and has an even number on it.

5. The event that the denomination of the chosen card is at least 10 (counting aces high).

6. The event that the denomination of the chosen card is at most 4 (counting aces high).

In 7–10, use the sample space given in Example 9.1.2. Write each of the following events as a set and compute its probability.

7. The event that the sum of the numbers showing face up is 8.

8. The event that the numbers showing face up are the same.

9. The event that the sum of the numbers showing face up is at most 6.

10. The event that the sum of the numbers showing face up is at least 9.

11. Suppose that a coin is tossed three times and the side showing face up on each toss is noted. Suppose also that on each toss heads and tails are equally likely. Let *HHT* indicate the outcome heads on the first two tosses and tails on the third, *THT* the outcome tails on the first and third tosses and heads on the second, and so forth.
    a. List the eight elements in the sample space whose outcomes are all the possible head-tail sequences obtained in the three tosses.
    b. Write each of the following events as a set and find its probability:
        (i) The event that exactly one toss results in a head.
        (ii) The event that at least two tosses result in a head.
        (iii) The event that no head is obtained.

12. Suppose that each child born is equally likely to be a boy or a girl. Consider a family with exactly three children. Let *BBG* indicate that the first two children born are boys and the third child is a girl, let *GBG* indicate that the first and third children born are girls and the second is a boy, and so forth.
    a. List the eight elements in the sample space whose outcomes are all possible genders of the three children.
    b. Write each of the events in the next column as a set and find its probability.
        (i) The event that exactly one child is a girl.
        (ii) The event that at least two children are girls.
        (iii) The event that no child is a girl.

13. Suppose that on a true/false exam you have no idea at all about the answers to three questions. You choose answers randomly and therefore have a 50–50 chance of being correct on any one question. Let *CCW* indicate that you were correct on the first two questions and wrong on the third, let *WCW* indicate that you were wrong on the first and third questions and correct on the second, and so forth.
    a. List the elements in the sample space whose outcomes are all possible sequences of correct and incorrect responses on your part.
    b. Write each of the following events as a set and find its probability:
        (i) The event that exactly one answer is correct.
        (ii) The event that at least two answers are correct.
        (iii) The event that no answer is correct.

14. Three people have been exposed to a certain illness. Once exposed, a person has a 50–50 chance of actually becoming ill.
    a. What is the probability that exactly one of the people becomes ill?

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

b. What is the probability that at least two of the people become ill?
c. What is the probability that none of the three people becomes ill?

15. When discussing counting and probability, we often consider situations that may appear frivolous or of little practical value, such as tossing coins, choosing cards, or rolling dice. The reason is that these relatively simple examples serve as models for a wide variety of more complex situations in the real world. In light of this remark, comment on the relationship between your answer to exercise 11 and your answers to exercises 12–14.

16. Two faces of a six-sided die are painted red, two are painted blue, and two are painted yellow. The die is rolled three times, and the colors that appear face up on the first, second, and third rolls are recorded.
a. Let *BBR* denote the outcome where the color appearing face up on the first and second rolls is blue and the color appearing face up on the third roll is red. Because there are as many faces of one color as of any other, the outcomes of this experiment are equally likely. List all 27 possible outcomes.
b. Consider the event that all three rolls produce different colors. One outcome in this event is *RBY* and another *RYB*. List all outcomes in the event. What is the probability of the event?
c. Consider the event that two of the colors that appear face up are the same. One outcome in this event is *RRB* and another is *RBR*. List all outcomes in the event. What is the probability of the event?

17. Consider the situation described in exercise 16.
a. Find the probability of the event that exactly one of the colors that appears face up is red.
b. Find the probability of the event that at least one of the colors that appears face up is red.

18. An urn contains two blue balls (denoted B_1 and B_2) and one white ball (denoted W). One ball is drawn, its color is recorded, and it is replaced in the urn. Then another ball is drawn, and its color is recorded.
a. Let B_1W denote the outcome that the first ball drawn is B_1 and the second ball drawn is W. Because the first ball is replaced before the second ball is drawn, the outcomes of the experiment are equally likely. List all nine possible outcomes of the experiment.
b. Consider the event that the two balls that are drawn are both blue. List all outcomes in the event. What is the probability of the event?
c. Consider the event that the two balls that are drawn are of different colors. List all outcomes in the event. What is the probability of the event?

19. An urn contains two blue balls (denoted B_1 and B_2) and three white balls (denoted W_1, W_2, and W_3). One ball is drawn, its color is recorded, and it is replaced in the urn. Then another ball is drawn and its color is recorded.
a. Let B_1W_2 denote the outcome that the first ball drawn is B_1 and the second ball drawn is W_2. Because the first ball is replaced before the second ball is drawn, the outcomes of the experiment are equally likely. List all 25 possible outcomes of the experiment.
b. Consider the event that the first ball that is drawn is blue. List all outcomes in the event. What is the probability of the event?
c. Consider the event that only white balls are drawn. List all outcomes in the event. What is the probability of the event?

*** 20.** Refer to Example 9.1.3. Suppose you are appearing on a game show with a prize behind one of five closed doors: A, B, C, D, and E. If you pick the correct door, you win the prize. You pick door A. The game show host then opens one of the other doors and reveals that there is no prize behind it. Then the host gives you the option of staying with your original choice of door A or switching to one of the other doors that is still closed.
a. If you stick with your original choice, what is the probability that you will win the prize?
b. If you switch to another door, what is the probability that you will win the prize?

21. a. How many positive two-digit integers are multiples of 3?
b. What is the probability that a randomly chosen positive two-digit integer is a multiple of 3?
c. What is the probability that a randomly chosen positive two-digit integer is a multiple of 4?

22. a. How many positive three-digit integers are multiples of 6?

b. What is the probability that a randomly chosen positive three-digit integer is a multiple of 6?
c. What is the probability that a randomly chosen positive three-digit integer is a multiple of 7?

23. Suppose $A[1], A[2], A[3], \ldots, A[n]$ is a one-dimensional array and $n > 50$.
a. How many elements are in the array?
b. How many elements are in the subarray

$$A[4], A[5], \ldots, A[39]?$$

c. If $3 \leq m \leq n$, what is the probability that a randomly chosen array element is in the subarray

$$A[3], A[4], \ldots, A[m]?$$

d. What is the probability that a randomly chosen array element is in the subarray shown below if $n = 39$?

$$A[\lfloor n/2 \rfloor], A[\lfloor n/2 \rfloor + 1], \ldots, A[n]$$

24. Suppose $A[1], A[2], \ldots, A[n]$ is a one-dimensional array and $n \geq 2$. Consider the subarray

$$A[1], A[2], \ldots, A[\lfloor n/2 \rfloor].$$

a. How many elements are in the subarray (i) if n is even? and (ii) if n is odd?
b. What is the probability that a randomly chosen array element is in the subarray (i) if n is even? and (ii) if n is odd?

25. Suppose $A[1], A[2], \ldots, A[n]$ is a one-dimensional array and $n \geq 2$. Consider the subarray

$$A[\lfloor n/2 \rfloor], A[\lfloor n/2 \rfloor + 1], \ldots, A[n].$$

a. How many elements are in the subarray (i) if n is even? and (ii) if n is odd?
b. What is the probability that a randomly chosen array element is in the subarray (i) if n is even? and (ii) if n is odd?

26. What is the 27th element in the one-dimensional array $A[42], A[43], \ldots, A[100]$?

27. What is the 62nd element in the one-dimensional array $B[29], B[30], \ldots, B[100]$?

28. If the largest of 56 consecutive integers is 279, what is the smallest?

29. If the largest of 87 consecutive integers is 326, what is the smallest?

30. How many even integers are between 1 and 1,001?

31. How many integers that are multiples of 3 are between 1 and 1,001?

32. A certain non-leap year has 365 days, and January 1 occurs on a Monday.
a. How many Sundays are in the year?
b. How many Mondays are in the year?

*** 33.** Prove Theorem 9.1.1. (Let m be any integer and prove the theorem by mathematical induction on n.)

ANSWERS FOR TEST YOURSELF

1. the set of all outcomes of the random process or experiment **2.** a subset of the sample space **3.** number of outcomes in the event; total number of outcomes **4.** $n - m + 1$

9.2 Possibility Trees and the Multiplication Rule

Don't believe anything unless you have thought it through for yourself.
—Anna Pell Wheeler, 1883–1966

A tree structure is a useful tool for keeping systematic track of all possibilities in situations in which events happen in order. The following example shows how to use such a structure to count the number of different outcomes of a tournament.

Example 9.2.1 Possibilities for Tournament Play

Teams A and B are to play each other repeatedly until one wins two games in a row or a total of three games. One way in which this tournament can be played is for A to win the

first game, B to win the second, and A to win the third and fourth games. Denote this by writing A–B–A–A.

a. How many ways can the tournament be played?

b. Assuming that all the ways of playing the tournament are equally likely, what is the probability that five games are needed to determine the tournament winner?

Solution

a. The possible ways for the tournament to be played are represented by the distinct paths from "root" (the start) to "leaf" (a terminal point) in the tree shown sideways in Figure 9.2.1. The label on each branching point indicates the winner of the game. The notations in parentheses indicate the winner of the tournament.

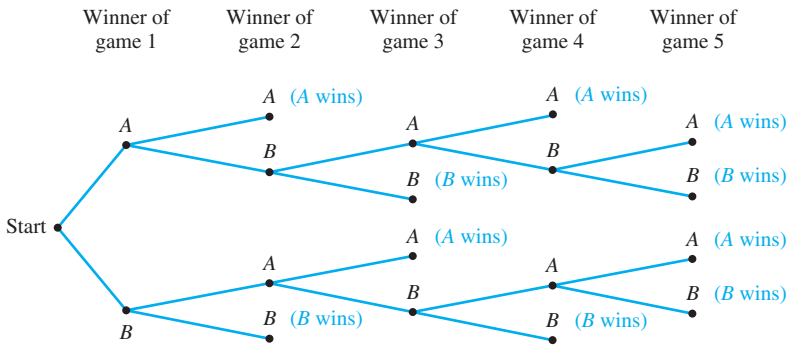


FIGURE 9.2.1 The Outcomes of a Tournament

The fact that there are ten paths from the root of the tree to its leaves shows that there are ten possible ways for the tournament to be played. They are (moving from the top down): A–A, A–B–A–A, A–B–A–B–A, A–B–A–B–B, A–B–B, B–A–A, B–A–B–A–A, B–A–B–A–B, B–A–B–B, and B–B. In five cases A wins, and in the other five B wins. The least number of games that must be played to determine a winner is two, and the most that will need to be played is five.

b. Since all the possible ways of playing the tournament listed in part (a) are assumed to be equally likely, and the listing shows that five games are needed in four different cases (A–B–A–B–A, A–B–A–B–B, B–A–B–A–B, and B–A–B–A–A), the probability that five games are needed is $4/10 = 2/5 = 40\%$. ■

The Multiplication Rule

Consider the following example. Suppose a computer installation has four input/output units (A, B, C, and D) and three central processing units (X, Y, and Z). Any input/output unit can be paired with any central processing unit. How many ways are there to pair an input/output unit with a central processing unit?

To answer this question, imagine the pairing of the two types of units as a two-step operation:

Step 1: Choose the input/output unit.

Step 2: Choose the central processing unit.

The possible outcomes of this operation are illustrated in the possibility tree of Figure 9.2.2.

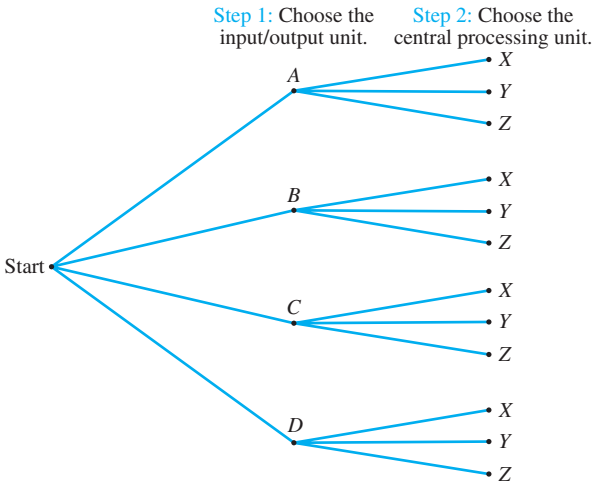


FIGURE 9.2.2 Pairing Objects Using a Possibility Tree

The topmost path from "root" to "leaf" indicates that input/output unit A is to be paired with central processing unit X. The next lower branch indicates that input/output unit A is to be paired with central processing unit Y. And so forth.

Thus the total number of ways to pair the two types of units is the same as the number of branches of the tree, which is

$$3 + 3 + 3 + 3 = 4 \cdot 3 = 12.$$

The idea behind this example can be used to prove the following rule. A formal proof uses mathematical induction and is left to the exercises.

Theorem 9.2.1 The Multiplication Rule

If an operation consists of k steps and

the first step can be performed in n_1 ways,

the second step can be performed in n_2 ways *[regardless of how the first step was performed]*,

$\vdots$

the kth step can be performed in n_k ways *[regardless of how the preceding steps were performed]*,

then the entire operation can be performed in $n_1 n_2 \cdots n_k$ ways.

To apply the multiplication rule, think of the objects you are trying to count as the output of a multistep operation. The possible ways to perform a step may depend on how preceding steps were performed, but the *number* of ways to perform each step must be constant regardless of the action taken in prior steps.

Example 9.2.2 **Counting Personal Identification Numbers (PINs)**

A certain personal identification number (PIN) is required to be a sequence of any four symbols chosen from the 26 uppercase letters in the Roman alphabet and the ten digits.

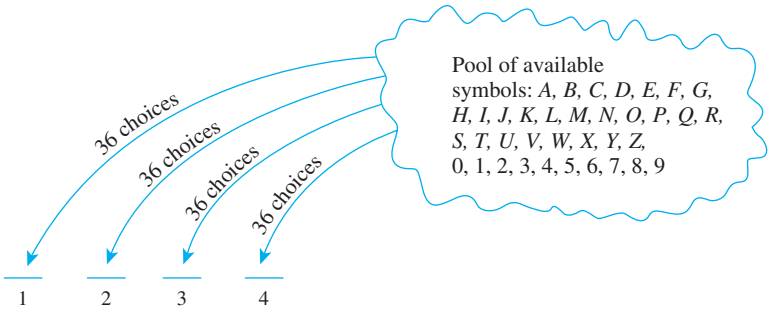
a. How many different PINs are possible if repetition of symbols is allowed?

b. How many different PINs are possible if repetition of symbols is not allowed?

c. What is the probability that a PIN does not have a repeated symbol assuming that all PINs are equally likely?

Solution

a. Some possible PINs are RCAE, 3387, B92B, and so forth. You can think of forming a PIN as a four-step operation where each step involves placing a symbol into one of four positions, as shown below.



Step 1: Choose a symbol to place in position 1.

Step 2: Choose a symbol to place in position 2.

Step 3: Choose a symbol to place in position 3.

Step 4: Choose a symbol to place in position 4.

There is a fixed number of ways to perform each step, namely 36, regardless of how preceding steps were performed. And so, by the multiplication rule, there are $36 \cdot 36 \cdot 36 \cdot 36 = 36^4 = 1{,}679{,}616$ PINs in all.

b. Again think of forming a PIN as a four-step operation: Choose the first symbol, then the second, then the third, and then the fourth. There are 36 ways to choose the first symbol, 35 ways to choose the second (since the first symbol cannot be used again), 34 ways to choose the third (since the first two symbols cannot be reused), and 33 ways to choose the fourth (since the first three symbols cannot be reused). Thus, the multiplication rule can be applied to conclude that there are $36 \cdot 35 \cdot 34 \cdot 33 = 1{,}413{,}720$ different PINs with no repeated symbol.

c. By part (b) there are 1,413,720 PINs with no repeated symbol, and by part (a) there are 1,679,616 PINs in all. Thus the probability that a PIN chosen at random contains no repeated symbol is $\frac{1{,}413{,}720}{1{,}679{,}616} \cong 0.8417$. In other words, approximately 84% of PINs have no repeated symbol. ■

Another way to look at the PINs of Example 9.2.2 is as ordered 4-tuples. For example, you can think of the PIN M2ZM as the ordered 4-tuple (M, 2, Z, M). Therefore, the total number of PINs is the same as the total number of ordered 4-tuples whose elements are either letters or digits. One of the most important uses of the multiplication rule is to derive a general formula for the number of elements in any Cartesian product of a finite number of finite sets. In Example 9.2.3, this is done for a Cartesian product of four sets.

Example 9.2.3 **The Number of Elements in a Cartesian Product**

Suppose A_1, A_2, A_3, and A_4 are sets with n_1, n_2, n_3, and n_4 elements, respectively. Show that the set $A_1 \times A_2 \times A_3 \times A_4$ has $n_1 n_2 n_3 n_4$ elements.

Solution Each element in $A_1 \times A_2 \times A_3 \times A_4$ is an ordered 4-tuple of the form (a_1, a_2, a_3, a_4), where $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$, and $a_4 \in A_4$. Imagine the process of constructing these ordered tuples as a four-step operation:

Step 1: Choose the first element of the 4-tuple.

Step 2: Choose the second element of the 4-tuple.

Step 3: Choose the third element of the 4-tuple.

Step 4: Choose the fourth element of the 4-tuple.

There are n_1 ways to perform step 1, n_2 ways to perform step 2, n_3 ways to perform step 3, and n_4 ways to perform step 4. Hence, by the multiplication rule, there are $n_1n_2n_3n_4$ ways to perform the entire operation. Therefore, there are $n_1n_2n_3n_4$ distinct 4-tuples in $A_1 \times A_2 \times A_3 \times A_4$. ■

Any circuit with two input signals P and Q has an input/output table consisting of four rows corresponding to the four possible assignments of values to P and Q: 11, 10, 01, and 00. The next example shows that there are only 16 distinct ways in which such a circuit can function.

Example 9.2.4 **Number of Input/Output Tables for a Circuit with Two Input Signals**

Consider the set of all circuits with two input signals P and Q. Each such circuit has a corresponding input/output table, but, as shown in Section 2.4, two such input/output tables may be the same. How many distinct input/output tables are there for a circuit with input/output signals P and Q?

Solution Fix the order of the input values for P and Q. Then two input/output tables are distinct if their output values differ in at least one row. For example, the input/output tables shown below are distinct, because their output values differ in the first row.

P	Q	Output
1	1	1
1	0	0
0	1	1
0	0	0

P	Q	Output
1	1	0
1	0	0
0	1	1
0	0	0

For a fixed ordering of input values, you can obtain a complete input/output table by filling in the entries in the output column. You can think of this as a four-step operation:

Step 1: Fill in the output value for the first row.

Step 2: Fill in the output value for the second row.

Step 3: Fill in the output value for the third row.

Step 4: Fill in the output value for the fourth row.

Each step can be performed in exactly two ways: either a 1 or a 0 can be filled in. Hence, by the multiplication rule, there are

$$2 \cdot 2 \cdot 2 \cdot 2 = 16$$

ways to perform the entire operation. It follows that there are $2^4 = 16$ distinct input/output tables for a circuit with two input signals P and Q. This means that such a circuit can function in only 16 distinct ways. ■

Observe that in Example 9.2.2, the set of all PINs of length 4 is the same as the set of all strings of length 4 over the set

$$S = \{x | x \text{ is a letter of the uppercase Roman alphabet or } x \text{ is a digit}\}.$$

Also observe that another way to think of Example 9.2.4 is to realize that there are as many input/output tables for a circuit with two input signals as there are bit strings of length 4 (written vertically) that can be used to fill in the output values. As another example, here is a listing of all bit strings of length 3:

$$000, \quad 001, \quad 010, \quad 100, \quad 011, \quad 101, \quad 110, \quad 111.$$

Example 9.2.5 **Counting the Number of Iterations of a Nested Loop**

Consider the following nested loop:

```
for i := 1 to 4
    for j := 1 to 3
        [Statements in body of inner loop.
        None contain branching statements
        that lead out of the inner loop.]
    next j
next i
```

How many times will the inner loop be iterated when the algorithm is implemented and run?

Solution The outer loop is iterated four times, and during each iteration of the outer loop, there are three iterations of the inner loop. Hence by the multiplication rule, the total number of iterations of the inner loop is $4 \cdot 3 = 12$. This is illustrated by the trace table below.

i	1			2			3			4		
j	1	2	3	1	2	3	1	2	3	1	2	3

$$3 + 3 + 3 + 3 = 12$$

■

When the Multiplication Rule Is Difficult or Impossible to Apply

Consider the following problem:

> Three officers—a president, a treasurer, and a secretary—are to be chosen from among four people: Ann, Bob, Cyd, and Dan. Suppose that, for various reasons, Ann cannot be president and either Cyd or Dan must be secretary. How many ways can the officers be chosen?

It is natural to try to solve this problem using the multiplication rule. A person might answer as follows:

> There are three choices for president (all except Ann), three choices for treasurer (all except the one chosen as president), and two choices for secretary (Cyd or Dan). Therefore, by the multiplication rule, there are $3 \cdot 3 \cdot 2 = 18$ choices in all.

Unfortunately, this analysis is incorrect. The number of ways to choose the secretary varies depending on who is chosen for president and treasurer. For instance, if Bob is chosen

for president and Ann for treasurer, then there are two choices for secretary: Cyd and Dan. But if Bob is chosen for president and Cyd for treasurer, then there is just one choice for secretary: Dan. The clearest way to see all the possible choices is to construct the possibility tree, as is shown in Figure 9.2.3.

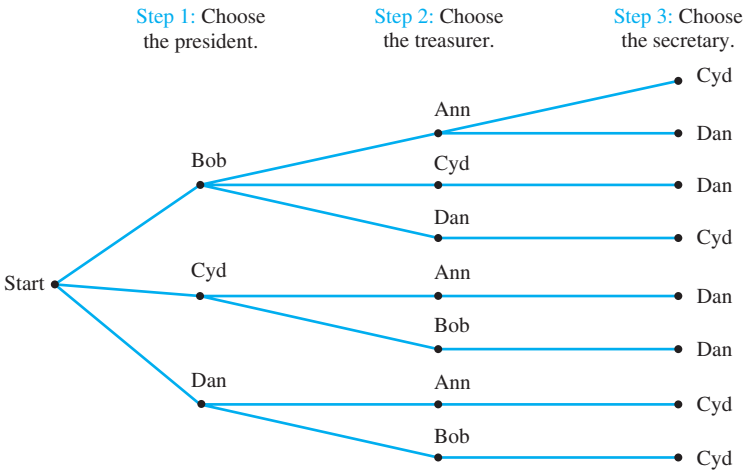


FIGURE 9.2.3

From the tree it is easy to see that there are only eight ways to choose a president, treasurer, and secretary so as to satisfy the given conditions.

Another way to solve this problem is somewhat surprising. It turns out that the steps can be reordered in a slightly different way so that the number of ways to perform each step is constant regardless of the way previous steps were performed.

Example 9.2.6 **A More Subtle Use of the Multiplication Rule**

Reorder the steps for choosing the officers in the previous example so that the total number of ways to choose officers can be computed using the multiplication rule.

Solution

Step 1: Choose the secretary.

Step 2: Choose the president.

Step 3: Choose the treasurer.

There are exactly two ways to perform step 1 (either Cyd or Dan may be chosen), two ways to perform step 2 (neither Ann nor the person chosen in step 1 may be chosen but either of the other two may), and two ways to perform step 3 (either of the two people not chosen as secretary or president may be chosen as treasurer). Thus, by the multiplication rule, the total number of ways to choose officers is $2 \cdot 2 \cdot 2 = 8$. A possibility tree illustrating this sequence of choices is shown in Figure 9.2.4. Note how balanced this tree is compared with the one in Figure 9.2.3.

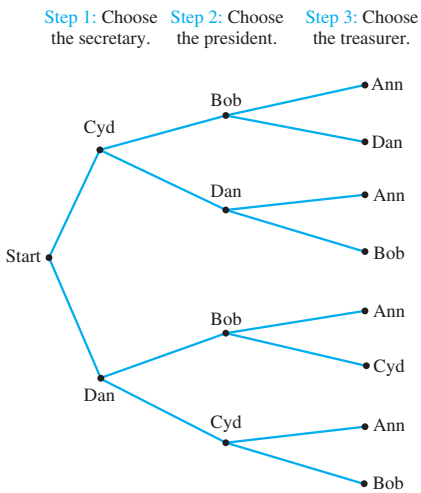


FIGURE 9.2.4

Permutations

A **permutation** of a set of objects is an ordering of the objects in a row. For example, the set of elements a, b, and c has six permutations.

$$abc \quad acb \quad cba \quad bac \quad bca \quad cab$$

In general, given a set of n objects, how many permutations does the set have? Imagine forming a permutation as an n-step operation:

Step 1: Choose an element to write first.
Step 2: Choose an element to write second.
⋮ ⋮
Step n: Choose an element to write nth.

Any element of the set can be chosen in step 1, so there are n ways to perform step 1. Any element except that chosen in step 1 can be chosen in step 2, so there are $n - 1$ ways to perform step 2. In general, the number of ways to perform each successive step is one less than the number of ways to perform the preceding step. At the point when the nth element is chosen, there is only one element left, so there is only one way to perform step n. Hence, by the multiplication rule, there are

$$n(n-1)(n-2)\cdots 2\cdot 1 = n!$$

ways to perform the entire operation. In other words, there are $n!$ permutations of a set of n elements. This reasoning is summarized in the following theorem. A formal proof uses mathematical induction and is left as an exercise.

Theorem 9.2.2

For any integer n with $n \geq 1$, the number of permutations of a set with n elements is $n!$.

Example 9.2.7 **Permutations of the Letters in a Word**

a. How many ways can the letters in the word *COMPUTER* be arranged in a row?

b. How many ways can the letters in the word *COMPUTER* be arranged if the letters *CO* must remain next to each other (in order) as a unit?

c. If letters of the word *COMPUTER* are randomly arranged in a row, what is the probability that the letters *CO* remain next to each other (in order) as a unit?

Solution

a. All eight letters in the word *COMPUTER* are distinct, so the number of ways in which you can arrange the letters equals the number of permutations of a set of eight elements. This equals $8! = 40{,}320$.

b. If the letter group *CO* is treated as a unit, then there are effectively only seven objects that are to be arranged in a row.

CO	M	P	U	T	E	R

Hence there are as many ways to write the letters as there are permutations of a set of seven elements, namely, $7! = 5{,}040$.

c. When the letters are arranged randomly in a row, the total number of arrangements is 40,320 by part (a), and the number of arrangements with the letters *CO* next to each other (in order) as a unit is 5,040. Thus the probability is

$$\frac{5{,}040}{40{,}320} = \frac{1}{8} = 12.5\%.$$ ■

Example 9.2.8 **Permutations of Objects Around a Circle**

At a meeting of diplomats, the six participants are to be seated around a circular table. Since the table has no ends to confer particular status, it doesn't matter who sits in which chair. But it does matter how the diplomats are seated relative to each other. In other words, two seatings are considered the same if one is a rotation of the other. How many different ways can the diplomats be seated?

Solution Call the diplomats by the letters A, B, C, D, E, and F. Since only relative position matters, you can start with any diplomat (say, A), place that diplomat anywhere (say, in the top seat of the diagram shown in Figure 9.2.5), and then consider all arrangements of the other diplomats around that one. The five diplomats B through F can be arranged in the seats around diplomat A in all possible orders. So there are $5! = 120$ ways to seat the group.

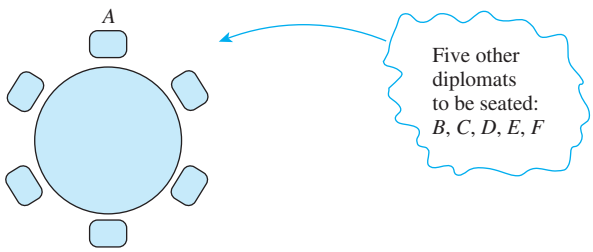


FIGURE 9.2.5 ■

Permutations of Selected Elements

Given the set $\{a, b, c\}$, there are six ways to select two letters from the set and write them in order.

$$ab \quad ac \quad ba \quad bc \quad ca \quad cb$$

Each such ordering of two elements of $\{a, b, c\}$ is called a 2-*permutation* of $\{a, b, c\}$.

Definition

An ***r*-permutation** of a set of n elements is an ordered selection of r elements taken from the set of n elements. The number of r-permutations of a set of n elements is denoted $\boldsymbol{P(n, r)}$.

Theorem 9.2.3

If n and r are integers and $1 \le r \le n$, then the number of r-permutations of a set of n elements is given by the formula

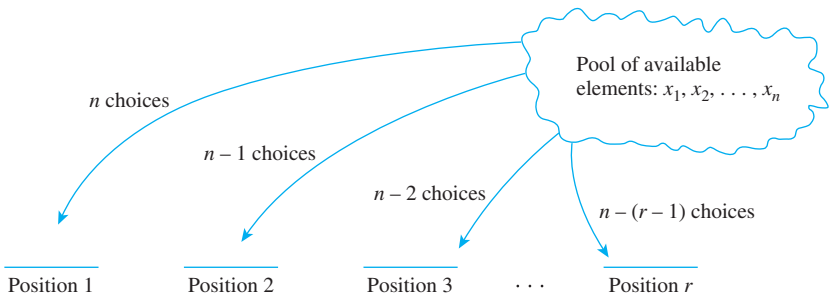
$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) \quad \text{first version}$$

or, equivalently,

$$P(n, r) = \frac{n!}{(n-r)!} \quad \text{second version.}$$

A formal proof of this theorem uses mathematical induction and is based on the multiplication rule. The idea of the proof is the following.

Suppose a set of n elements is given. Formation of an r-permutation can be thought of as an r-step process. Step 1 is to choose the element to be first. Since the set has n elements, there are n ways to perform step 1. Step 2 is to choose the element to be second. Since the element chosen in step 1 is no longer available, there are $n-1$ ways to perform step 2. Step 3 is to choose the element to be third. Since neither of the two elements chosen in the first two steps is available, there are $n-2$ choices for step 3. This process is repeated r times, as shown below.



The number of ways to perform each successive step is one less than the number of ways to perform the preceding step. Step r is to choose the element to be rth. At the point just before step r is performed, $r-1$ elements have already been chosen, and so there are

$$n-(r-1) = n-r+1$$

left to choose from. Hence there are $n-r+1$ ways to perform step r. It follows by the multiplication rule that the number of ways to form an r-permutation is

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1).$$

Note that

$$\begin{aligned}\frac{n!}{(n-r)!} &= \frac{n(n-1)(n-2)\cdots(n-r+1)\cancel{(n-r)}\cancel{(n-r-1)}\cdots\cancel{3}\cdot\cancel{2}\cdot\cancel{1}}{\cancel{(n-r)}\cancel{(n-r-1)}\cdots\cancel{3}\cdot\cancel{2}\cdot\cancel{1}} \\ &= n(n-1)(n-2)\cdots(n-r+1).\end{aligned}$$

Thus the formula can also be written as

$$P(n, r) = \frac{n!}{(n-r)!}.$$

The second version of the formula is easier to remember, but if you use it with a calculator, don't first compute $n!$ and $(n-r)!$ and then divide the first by the second. Because factorials become so large so fast, using this method can overload a calculator's capacity for exact arithmetic even when n and r are quite small. For instance, if $n = 15$ and $r = 2$, then

$$\frac{n!}{(n-r)!} = \frac{15!}{13!} = \frac{1{,}307{,}674{,}368{,}000}{6{,}227{,}020{,}800}.$$

On the other hand, if you cancel $(n-r)! = 13!$ from the numerator and denominator before multiplying out, you reduce the expression to the first version of the formula for $P(n, r)$, which is much easier to compute:

$$\frac{n!}{(n-r)!} = \frac{15!}{13!} = \frac{15 \cdot 14 \cdot \cancel{13!}}{\cancel{13!}} = 15 \cdot 14 = 210.$$

In fact, many scientific calculators allow you to compute $P(n, r)$ simply by entering the values of n and r and pressing a key or making a menu choice. Alternative notations for $P(n, r)$ are ${}_n P_r$, $P_{n,r}$, and ${}^n P_r$.

Example 9.2.9 **Evaluating *r*-Permutations**

a. Evaluate $P(5, 2)$.

b. How many 4-permutations are there of a set of seven objects?

c. How many 5-permutations are there of a set of five objects?

Solution

a. $$P(5, 2) = \frac{5!}{(5-2)!} = \frac{5 \cdot 4 \cdot \cancel{3!}}{\cancel{3!}} = 20$$

b. The number of 4-permutations of a set of seven objects is

$$P(7, 4) = \frac{7!}{(7-4)!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot \cancel{3!}}{\cancel{3!}} = 7 \cdot 6 \cdot 5 \cdot 4 = 840.$$

c. The number of 5-permutations of a set of five objects is

$$P(5, 5) = \frac{5!}{(5-5)!} = \frac{5!}{0!} = \frac{5!}{1} = 5! = 120.$$

Note that the definition of 0! as 1 makes this calculation come out as it should, for the number of 5-permutations of a set of five objects is certainly equal to the number of permutations of the set. ■

Example 9.2.10 **Permutations of Selected Letters of a Word**

a. How many different ways can three of the letters of the word *BYTES* be chosen and written in a row?

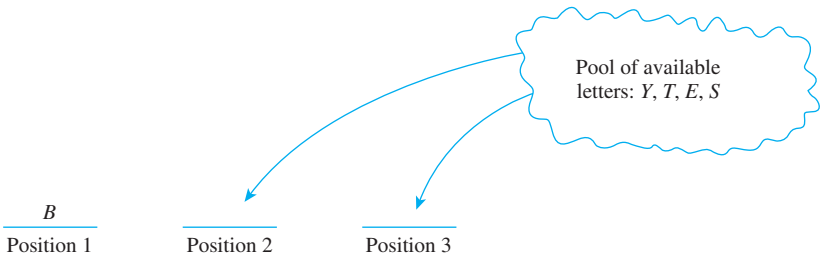
b. How many different ways can this be done if the first letter must be *B*?

Solution

a. The answer equals the number of 3-permutations of a set of five elements. This equals

$$P(5, 3) = \frac{5!}{(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot \cancel{2!}}{\cancel{2!}} = 5 \cdot 4 \cdot 3 = 60.$$

b. Since the first letter must be B, there are effectively only two letters to be chosen and placed in the other two positions. And since the B is used in the first position, there are four letters available to fill the remaining two positions.



Hence the answer is the number of 2-permutations of a set of four elements, which is

$$P(4, 2) = \frac{4!}{(4-2)!} = \frac{4 \cdot 3 \cdot 2!}{2!} = 4 \cdot 3 = 12.$$ ■

In many applications of the mathematics of counting, it is necessary to be skillful in working algebraically with quantities of the form $P(n, r)$. The next example shows a kind of problem that gives practice in developing such skill.

Example 9.2.11 **Proving a Property of $P(n, r)$**

Prove that for every integer $n \geq 2$,

$$P(n, 2) + P(n, 1) = n^2.$$

Solution Suppose n is any integer that is greater than or equal to 2. By Theorem 9.2.3,

$$P(n, 2) = \frac{n!}{(n-2)!} = \frac{n(n-1)(n-2)!}{(n-2)!} = n(n-1)$$

and

$$P(n, 1) = \frac{n!}{(n-1)!} = \frac{n \cdot (n-1)!}{(n-1)!} = n.$$

Hence

$$P(n, 2) + P(n, 1) = n \cdot (n-1) + n = n^2 - n + n = n^2,$$

which is what we needed to show. ■

TEST YOURSELF

1. The multiplication rule says that if an operation can be performed in k steps and, for each i with $1 \leq i \leq k$, the ith step can be performed in n_i ways (regardless of how previous steps were performed), then the operation as a whole can be performed in _____.
2. A permutation of a set of elements is _____.
3. The number of permutations of a set of n elements equals _____.
4. An r-permutation of a set of n elements is _____.
5. The number of r-permutations of a set of n elements is denoted _____.
6. One formula for the number of r-permutations of a set of n elements is _____ and another formula is _____.

EXERCISE SET 9.2

In 1–4, use the fact that in baseball's World Series, the first team to win four games wins the series.

1. Suppose team A wins the first three games. How many ways can the World Series be completed? (Draw a tree.)
2. Suppose team A wins the first two games. How many ways can the World Series be completed? (Draw a tree.)
3. How many ways can a World Series be played if team A wins four games in a row?
4. How many ways can a World Series be played if no team wins two games in a row?
5. In a competition between players X and Y, the first player to win three games in a row or a total of four games wins. How many ways can the competition be played if X wins the first game and Y wins the second and third games? (Draw a tree.)
6. One urn contains two black balls (labeled B_1 and B_2) and one white ball. A second urn contains one black ball and two white balls (labeled W_1 and W_2). Suppose the following experiment is performed: One of the two urns is chosen at random. Next a ball is randomly chosen from the urn. Then a second ball is chosen at random from the same urn without replacing the first ball.
   a. Construct the possibility tree showing all possible outcomes of this experiment.
   b. What is the total number of outcomes of this experiment?
   c. What is the probability that two black balls are chosen?
   d. What is the probability that two balls of opposite color are chosen?
7. One urn contains one blue ball (labeled B_1) and three red balls (labeled R_1, R_2, and R_3). A second urn contains two red balls (R_4 and R_5) and two blue balls (B_2 and B_3). An experiment is performed in which one of the two urns is chosen at random and then two balls are randomly chosen from it, one after the other without replacement.
   a. Construct the possibility tree showing all possible outcomes of this experiment.
   b. What is the total number of outcomes of this experiment?
   c. What is the probability that two red balls are chosen?
8. A person buying a personal computer system is offered a choice of three models of the basic unit, two models of keyboard, and two models of printer. How many distinct systems can be purchased?
9. Suppose there are three roads from city A to city B and five roads from city B to city C.
   a. How many ways is it possible to travel from city A to city C via city B?
   b. How many different round-trip routes are there from city A to B to C to B and back to A?
   c. How many different routes are there from cities A to B to C to B and back to A in which no road is traversed twice?
10. Suppose there are three routes from North Point to Boulder Creek, two routes from Boulder Creek to Beaver Dam, two routes from Beaver Dam to Star Lake, and four routes directly from Boulder Creek to Star Lake. (Draw a sketch.)
    a. How many routes from North Point to Star Lake pass through Beaver Dam?
    b. How many routes from North Point to Star Lake bypass Beaver Dam?
11. a. A bit string is a finite sequence of 0's and 1's. How many bit strings have length 8?
    b. How many bit strings of length 8 begin with three 0's?
    c. How many bit strings of length 8 begin and end with a 1?
12. Hexadecimal numbers are made using the sixteen hexadecimal digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F and are denoted using the subscript 16. For example, $9A2D_{16}$ and $BC54_{16}$ are hexadecimal numbers.
    a. How many hexadecimal numbers begin with one of the digits 3 through B, end with one of the digits 5 through F, and are 5 digits long?
    b. How many hexadecimal numbers begin with one of the digits 4 through D, end with one of the digits 2 through E, and are 6 digits long?
13. A coin is tossed four times. Each time the result H for heads or T for tails is recorded. An outcome of $HHTT$ means that heads were obtained on the first two tosses and tails on the second two. Assume that heads and tails are equally likely on each toss.
    a. How many distinct outcomes are possible?
    b. What is the probability that exactly two heads occur?

c. What is the probability that exactly one head occurs?

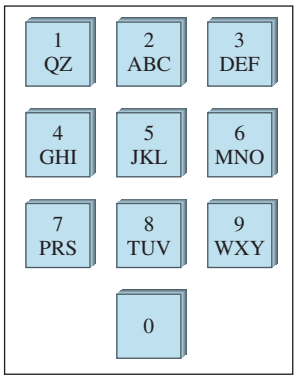
14. Suppose that in a certain state, all automobile license plates have four uppercase letters followed by three digits.
- **a.** How many different license plates are possible?
- **b.** How many license plates could begin with *A* and end in 0?
- **c.** How many license plates could begin with *TGIF*?
- **d.** How many license plates are possible in which all the letters and digits are distinct?
- **e.** How many license plates could begin with *AB* and have all letters and digits distinct?

15. A combination lock requires three selections of numbers, each from 1 through 30.
- **a.** How many different combinations are possible?
- **b.** Suppose the locks are constructed in such a way that no number may be used twice. How many different combinations are possible?

16.
- **a.** How many integers are there from 10 through 99?
- **b.** How many odd integers are there from 10 through 99?
- **c.** How many integers from 10 through 99 have distinct digits?
- **d.** How many odd integers from 10 through 99 have distinct digits?
- **e.** What is the probability that a randomly chosen two-digit integer has distinct digits? has distinct digits and is odd?

17.
- **a.** How many integers are there from 1000 through 9999?
- **b.** How many odd integers are there from 1000 through 9999?
- **c.** How many integers from 1000 through 9999 have distinct digits?
- **d.** How many odd integers from 1000 through 9999 have distinct digits?
- **e.** What is the probability that a randomly chosen four-digit integer has distinct digits? has distinct digits and is odd?

18. The following diagram shows the keypad for an automatic teller machine. As you can see, the same sequence of keys represents a variety of different PINs. For instance, 2133, AZDE, and BQ3F are all keyed in exactly the same way.



- **a.** How many different PINs are represented by the same sequence of keys as 2133?
- **b.** How many different PINs are represented by the same sequence of keys as 5031?
- **c.** How many different numeric sequences on the machine contain no repeated digit?

19. Three officers—a president, a treasurer, and a secretary—are to be chosen from among four people: Ann, Bob, Cyd, and Dan. Suppose that Bob is not qualified to be treasurer and Cyd's other commitments make it impossible for her to be secretary. How many ways can the officers be chosen? Can the multiplication rule be used to solve this problem?

20. Modify Example 9.2.4 by supposing that a PIN must not begin with any of the letters A–M and must end with a digit. Continue to assume that no symbol may be used more than once and that the total number of PINs is to be determined.

- **a.** Find the error in the following "solution."

"Constructing a PIN is a four-step process.

Step 1: Choose the left-most symbol.

Step 2: Choose the second symbol from the left.

Step 3: Choose the third symbol from the left.

Step 4: Choose the right-most symbol.

Because none of the thirteen letters from A through M may be chosen in step 1, there are $36 - 13 = 23$ ways to perform step 1. There are 35 ways to perform step 2 and 34 ways to perform step 3 because previously used symbols may not be used. Since the symbol chosen in step 4 must be a previously unused digit,

there are $10 - 3 = 7$ ways to perform step 4. Thus there are $23 \cdot 35 \cdot 34 \cdot 7 = 191{,}590$ different PINs that satisfy the given conditions."

b. Reorder steps 1–4 in part (a) as follows:

Step 1: Choose the right-most symbol.

Step 2: Choose the left-most symbol.

Step 3: Choose the second symbol from the left.

Step 4: Choose the third symbol from the left.

Use the multiplication rule to find the number of PINs that satisfy the given conditions.

H 21. Suppose A is a set with m elements and B is a set with n elements.

a. How many relations are there from A to B? Explain.

b. How many functions are there from A to B? Explain.

c. What fraction of the relations from A to B are functions?

22. a. How many functions are there from a set with three elements to a set with four elements?

b. How many functions are there from a set with five elements to a set with two elements?

c. How many functions are there from a set with m elements to a set with n elements, where m and n are positive integers?

23. In Section 2.5 we showed how integers can be represented by strings of 0's and 1's inside a digital computer. In fact, through various coding schemes, strings of 0's and 1's can be used to represent all kinds of symbols. One commonly used code is the Extended Binary-Coded Decimal Interchange Code (EBCDIC) in which each symbol has an 8-bit representation. How many distinct symbols can be represented by this code?

In each of 24–28, determine how many times the innermost loop will be iterated when the algorithm segment is implemented and run. (Assume that *m*, *n*, *p*, *a*, *b*, *c*, and *d* are all positive integers.)

24.
```
for i := 1 to 30
    for j := 1 to 15
        [Statements in body of inner loop.
        None contain branching statements that
        lead outside the loop.]
    next j
next i
```

25.
```
for j := 1 to m
    for k := 1 to n
        [Statements in body of inner loop.
        None contain branching statements that
        lead outside the loop.]
    next k
next j
```

26.
```
for i := 1 to m
    for j := 1 to n
        for k := 1 to p
            [Statements in body of inner loop.
            None contain branching statements
            that lead outside the loop.]
        next k
    next j
next i
```

27.
```
for i := 5 to 50
    for j := 10 to 20
        [Statements in body of inner loop.
        None contain branching statements that
        lead outside the loop.]
    next j
next i
```

28. Assume $a \le b$ and $c \le d$.
```
for i := a to b
    for j := c to d
        [Statements in body of inner loop.
        None contain branching statements that
        lead outside the loop.]
    next j
next i
```

H* 29. Consider the numbers 1 through 99,999 in their ordinary decimal representations. How many contain exactly one of each of the digits 2, 3, 4, and 5?

***30.** Let $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ where $p_1, p_2, \ldots, p_m$ are distinct prime numbers and $k_1, k_2, \ldots, k_m$ are positive integers. How many ways can n be written as a product of two positive integers that have no common factors, assuming the following?

a. Order matters (that is, $8 \cdot 15$ and $15 \cdot 8$ are regarded as different).

b. Order does not matter (that is, $8 \cdot 15$ and $15 \cdot 8$ are regarded as the same).

*31. a. If p is a prime number and a is a positive integer, how many distinct positive divisors does p^a have?
b. If p and q are distinct prime numbers and a and b are positive integers, how many distinct positive divisors does $p^a q^b$ have?
c. If p, q, and r are distinct prime numbers and a, b, and c are positive integers, how many distinct positive divisors does $p^a q^b r^c$ have?
d. If $p_1, p_2, \ldots, p_m$ are distinct prime numbers and $a_1, a_2, \ldots, a_m$ are positive integers, how many distinct positive divisors does $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ have?
e. What is the smallest positive integer with exactly 12 divisors?

32. a. How many ways can the letters of the word *ALGORITHM* be arranged in a row?
b. How many ways can the letters of the word *ALGORITHM* be arranged in a row if *A* and *L* must remain together (in order) as a unit?
c. How many ways can the letters of the word *ALGORITHM* be arranged in a row if the letters *GOR* must remain together (in order) as a unit?

33. Six people attend the theater together and sit in a row with exactly six seats.
a. How many ways can they be seated together in the row?
b. Suppose one of the six is a doctor who must sit on the aisle in case she is paged. How many ways can the people be seated together in the row with the doctor in an aisle seat?
c. Suppose the six people consist of three married couples and each couple wants to sit together with the older partner on the left. How many ways can the six be seated together in the row?

34. Five people are to be seated around a circular table. Two seatings are considered the same if one is a rotation of the other. How many different seatings are possible?

35. Write all the 2-permutations of $\{W, X, Y, Z\}$.

36. Write all the 3-permutations of $\{s, t, u, v\}$.

37. Evaluate the following quantities.
a. $P(6, 4)$ b. $P(6, 6)$ c. $P(6, 3)$ d. $P(6, 1)$

38. a. How many 3-permutations are there of a set of five objects?
b. How many 2-permutations are there of a set of eight objects?

39. a. How many ways can three of the letters of the word *ALGORITHM* be selected and written in a row?
b. How many ways can six of the letters of the word *ALGORITHM* be selected and written in a row?
c. How many ways can six of the letters of the word *ALGORITHM* be selected and written in a row if the first letter must be *A*?
d. How many ways can six of the letters of the word *ALGORITHM* be selected and written in a row if the first two letters must be *OR*?

40. Prove that for every integer $n \geq 2$, $P(n + 1, 3) = n^3 - n$.

41. Prove that for every integer $n \geq 2$,
$$P(n + 1, 2) - P(n, 2) = 2P(n, 1).$$

42. Prove that for every integer $n \geq 3$,
$$P(n + 1, 3) - P(n, 3) = 3P(n, 2).$$

43. Prove that for every integer $n \geq 2$, $P(n, n) = P(n, n - 1)$.

44. Prove Theorem 9.2.1 by mathematical induction.

H 45. Prove Theorem 9.2.2 by mathematical induction.

*46. Prove Theorem 9.2.3 by mathematical induction.

47. A permutation on a set can be regarded as a function from the set to itself. For instance, one permutation of $\{1, 2, 3, 4\}$ is 2341. It can be identified with the function that sends each position number to the number occupying that position. Since position 1 is occupied by 2, 1 is sent to 2 or $1 \longrightarrow 2$; since position 2 is occupied by 3, 2 is sent to 3 or $2 \longrightarrow 3$; and so forth. The entire permutation can be written using arrows as follows:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

a. Use arrows to write each of the six permutations of $\{1, 2, 3\}$.
b. Use arrows to write each of the permutations of $\{1, 2, 3, 4\}$ that keep 2 and 4 fixed.
c. Which permutations of $\{1, 2, 3\}$ keep no elements fixed?
d. Use arrows to write all permutations of $\{1, 2, 3, 4\}$ that keep no elements fixed.

ANSWERS FOR TEST YOURSELF

1. $n_1 n_2 \cdots n_k$ ways **2.** an ordering of the elements of the set in a row **3.** $n!$ **4.** an ordered selection of r of the elements of the set **5.** $P(n, r)$ **6.** $n(n-1)(n-2)\cdots(n-r+1)$; $\dfrac{n!}{(n-r)!}$

9.3 Counting Elements of Disjoint Sets: The Addition Rule

The whole of science is nothing more than a refinement of everyday thinking.
—Albert Einstein, 1879–1955

In the last section we discussed counting problems that can be solved using possibility trees. In this section we look at counting problems that can be solved by counting the number of elements in the union of two sets, the difference of two sets, or the intersection of two sets.

The basic rule underlying the calculation of the number of elements in a union or difference or intersection is the addition rule. This rule states that the number of elements in a union of mutually disjoint finite sets equals the sum of the number of elements in each of the component sets.

Theorem 9.3.1 The Addition Rule

Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then

$$N(A) = N(A_1) + N(A_2) + \cdots + N(A_k).$$

A formal proof of this theorem uses mathematical induction and is left to the exercises.

Example 9.3.1 **Counting the Number of Integers Divisible by 5**

How many three-digit integers (integers from 100 to 999 inclusive) are divisible by 5?

Solution One solution to this problem was discussed in Example 9.1.4. Another approach uses the addition rule. Integers that are divisible by 5 end either in 5 or in 0. Thus the set of all three-digit integers that are divisible by 5 can be split into two mutually disjoint subsets A_1 and A_2 as shown in Figure 9.3.1.

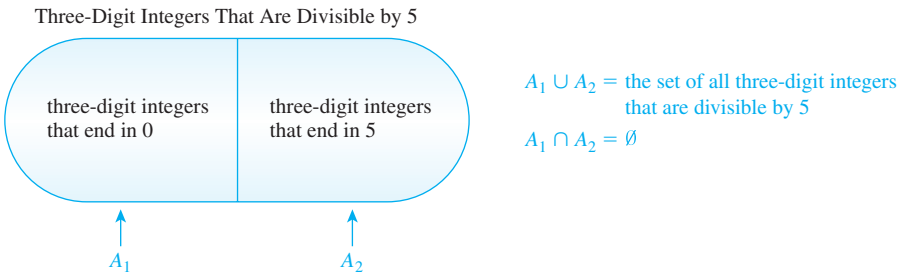


FIGURE 9.3.1

Now there are as many three-digit integers that end in 0 as there are possible choices for the left-most and middle digits (because the right-most digit must be a 0). As illustrated

below, there are nine choices for the left-most digit (the digits 1 through 9) and ten choices for the middle digit (the digits 0 through 9). Hence $N(A_1) = 9 \cdot 10 = 90$.

$$\underset{\substack{\uparrow \\ \text{9 choices} \\ \text{1, 2, 3, 4, 5, 6, 7, 8, 9}}}{\square} \qquad \underset{\substack{\uparrow \\ \text{10 choices} \\ \text{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}}}{\square} \qquad \underset{\substack{\uparrow \\ \text{number ends in 0}}}{\square}$$

Similar reasoning shows that there are as many three-digit integers that end in 5 as there are possible choices for the left-most and middle digits, which are the same as for the integers that end in 0. Hence, $N(A_2) = 90$. So

$$\begin{bmatrix} \text{the number of} \\ \text{three-digit integers} \\ \text{that are divisible by 5} \end{bmatrix} = N(A_1) + N(A_2) = 90 + 90 = 180.$$ ■

The Difference Rule

An important consequence of the addition rule is the fact that if the number of elements in a set A and the number in a subset B of A are both known, then the number of elements that are in A and not in B can be computed.

Theorem 9.3.2 The Difference Rule

If A is a finite set and B is a subset of A, then

$$N(A - B) = N(A) - N(B).$$

The difference rule is illustrated in Figure 9.3.2.

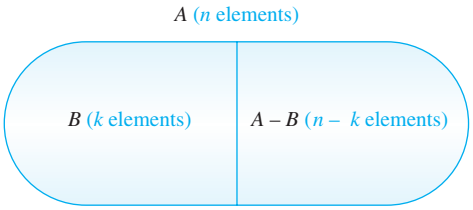


FIGURE 9.3.2 The Difference Rule

The difference rule holds for the following reason: If B is a subset of A, then the two sets B and $A - B$ have no elements in common and $B \cup (A - B) = A$. Hence, by the addition rule,

$$N(B) + N(A - B) = N(A).$$

Subtracting $N(B)$ from both sides gives the equation

$$N(A - B) = N(A) - N(B).$$

Example 9.3.2 **Counting PINs with Repeated Symbols**

Consider again the PINs discussed in Example 9.2.2. These are made from exactly four symbols chosen from the 26 uppercase letters of the Roman alphabet and the ten digits.

Example 9.2.2 showed that there are 1,679,616 PINs with repetition allowed and 265,896 PINs with no repeated symbol.

a. How many PINs contain at least one repeated symbol?

b. If all PINs are equally likely, what is the probability that a randomly chosen PIN contains at least one repeated symbol?

Solution

a. Let S be the set of all the PINs with repetition allowed, and let A be the set of PINs with no repeated symbol. Then $S - A$ is the set of PINs with at least one repeated symbol, and, by the difference rule,

$$\begin{aligned} N(S - A) &= N(S) - N(A) \\ &= 1{,}679{,}616 - 1{,}413{,}720 \\ &= 265{,}896. \end{aligned}$$

Hence, there are 265,896 PINs that contain at least one repeated symbol.

b. *Solution* 1: Because there are 1,679,616 PINs in all and 265,896 of these contain at least one repeated symbol, by the equally likely probability formula, the probability that a randomly chosen PIN contains a repeated symbol is

$$\frac{265{,}896}{1{,}679{,}616} \cong 0.158 = 15.8\%.$$

Solution 2: $P(A)$ is the probability that a randomly chosen PIN has no repeated symbol, and so $P(S - A)$ is the probability that a randomly chosen PIN has at least one repeated symbol. Then

$$\begin{aligned} P(S - A) &= \frac{N(S - A)}{N(S)} && \text{by definition of probability in the equally likely case} \\ &= \frac{N(S) - N(A)}{N(S)} && \text{by the difference rule} \\ &= \frac{N(S)}{N(S)} - \frac{N(A)}{N(S)} && \text{by the laws of fractions} \\ &= 1 - P(A) && \text{by definition of probability in the equally likely case} \\ &\cong 1 - 0.842 && \text{by Example 9.2.2} \\ &\cong 0.158 = 15.8\%. \end{aligned}$$

■

Solution 2 illustrates a general property of probabilities: that the probability of the complement of an event is obtained by subtracting the probability of the event from the number 1. In Section 9.8 we derive this formula from the axioms for probability.

Formula for the Probability of the Complement of an Event

If S is a finite sample space and A is an event in S, then

$$P(A^c) = 1 - P(A),$$

where $A^c = S - A$, the complement of A in S.

Example 9.3.3 **Passwords with 3–5 Letters**

A certain computer access password consists of 3 through 5 uppercase letters chosen from the 26 letters in the Roman alphabet, with repetitions allowed.

a. How many different passwords are possible?

b. How many different passwords have no repeated letter?

c. How many different passwords have at least one repeated letter?

d. If all passwords are equally likely, what is the probability that a randomly chosen password has at least one repeated letter?

Solution

a. The set of all passwords can be partitioned into three subsets consisting of passwords with lengths 3, 4, and 5, as shown in Figure 9.3.3.

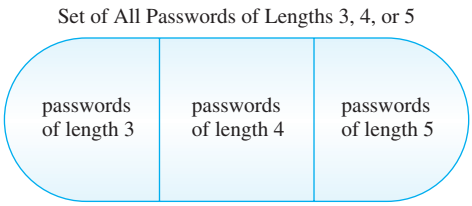


FIGURE 9.3.3

By the addition rule, the total number of passwords equals the number with length 3, plus the number with length 4, plus the number with length 5. The multiplication rule can be used to compute the number of passwords of each length. Thus the

$$\text{number of passwords with length } 3 = 26^3$$ because forming such a password can be thought of as a three-step process with 26 ways to perform each step

$$\text{number of passwords with length } 4 = 26^4$$ because forming such a password can be thought of as a four-step process with 26 ways to perform each step

$$\text{number of passwords with length } 5 = 26^5$$ because forming such a password can be thought of as a five-step process with 26 ways to perform each step.

Hence the total number of passwords is

$$26^3 + 26^4 + 26^5 = 12{,}355{,}928.$$

b. Constructing a password with length 3 and no repeated letter is a three-step process with 26 choices for step 1, 25 choices for step 2, and 24 choices for step 3. Thus there are $26 \cdot 25 \cdot 24$ passwords with length three and no repeated letter. Similarly, there are $26 \cdot 25 \cdot 24 \cdot 23$ passwords with length 4 and no repeated letter and $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22$ passwords with length 5 and no repeated letter. Hence the total number of passwords with no repeated letter is

$$26 \cdot 25 \cdot 24 + 26 \cdot 25 \cdot 24 \cdot 23 + 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 8{,}268{,}000.$$

c. By part (a) the total number of passwords is 12,355,928, and by part (b) 8,268,000 of these passwords do not have a repeated letter. Thus, by difference rule, the number of passwords with at least one repeated letter is 4,087,928.

d. Given the assumption that all passwords are equally likely, the equally likely probability formula can be used. So the probability that a randomly chosen password has at least one repeated letter is

$$\frac{\begin{bmatrix}\text{\# of passwords with}\\ \text{no repeated letter}\end{bmatrix}}{\text{total \# of passwords}} = \frac{4{,}087{,}928}{12{,}355{,}928} \cong 33.1\%. \quad \blacksquare$$

Example 9.3.4 **Number of Python Identifiers of Eight or Fewer Characters**

In the computer language Python, identifiers must start with one of 53 symbols: either one of the 52 letters of the upper- and lower-case Roman alphabet or an underscore (_). The initial character may stand alone, or it may be followed by any number of additional characters chosen from a set of 63 symbols: the 53 symbols allowed as an initial character plus the ten digits. Certain keywords, however, such as *and*, *if*, *print*, and so forth, are set aside and may not be used as identifiers. In one implementation of Python there are 31 such reserved keywords, none of which has more than eight characters. How many Python identifiers are there that are less than or equal to eight characters in length?

Solution The set of all Python identifiers with eight or fewer characters can be partitioned into eight subsets—identifiers of length 1, identifiers of length 2, and so on—as shown in Figure 9.3.4. The reserved words have various lengths (all less than or equal to 8), so the set of reserved words is shown overlapping the various subsets.

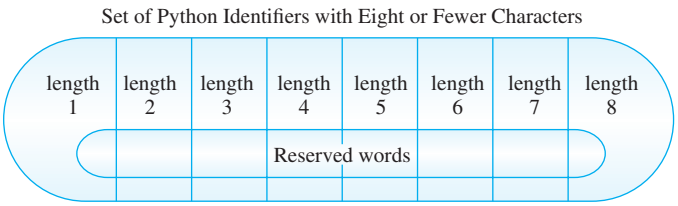


FIGURE 9.3.4

According to the rules for creating Python identifiers, there are

53 potential identifiers of length 1	because there are 53 choices for the first character
$53 \cdot 63$ potential identifiers of length 2	because the first character can be any one of 53 symbols, and the second character can be any one of 63 symbols
$53 \cdot 63^2$ potential identifiers of length 3	because the first character can be any one of 53 symbols, and each of the next two characters can be any one of 63 symbols
⋮	
$53 \cdot 63^7$ potential identifiers of length 8	because the first character can be any one of 53 symbols, and each of the next seven characters can be any one of 63 symbols.

Thus, by the addition rule, the number of potential Python identifiers with eight or fewer characters is

$$\begin{aligned} 53 + 53\cdot 63 + 53\cdot 63^2 + 53\cdot 63^3 + 53\cdot 63^4 + 53\cdot 63^5 + 53\cdot 63^6 + 53\cdot 63^7 & \\ = 53\left(\frac{63^8 - 1}{63 - 1}\right) & \text{ by Theorem 5.2.2} \\ = 212{,}133{,}167{,}002{,}880. & \end{aligned}$$

Now 31 of these potential identifiers are reserved, so by the difference rule, the actual number of Python identifiers with eight or fewer characters is

$$212{,}133{,}167{,}002{,}880 - 31 = 212{,}133{,}167{,}002{,}849. \quad \blacksquare$$

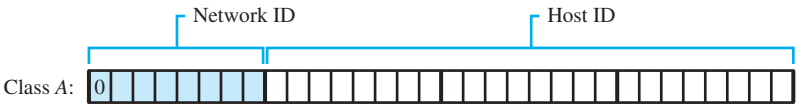
Example 9.3.5 **Internet Addresses**

In order to communicate effectively, each computer in a network needs a distinguishing name called an address. For the Internet this address is currently a 32-bit number called the Internet Protocol (IP) address (although 128-bit addresses are being phased in to accommodate the growth of the Internet). For technical reasons some computers have more than one address, whereas other sets of computers, which use the Internet only sporadically, may share a pool of addresses that are assigned on a temporary basis. Like telephone numbers, IP addresses are divided into parts: one, the network ID, specifies the local network to which a given computer belongs, and the other, the host ID, specifies the particular computer.

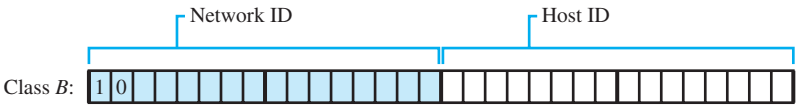
An example of an IP address is 10001100 11000000 00100000 10001000, where the 32 bits have been divided into four groups of 8 for easier reading. To make the reading even easier, IP addresses are normally written as "dotted decimals," in which each group of 8 bits is converted into a decimal number between 0 and 255. For instance, the IP address above converts into 140.192.32.136.

In order to accommodate the various sizes of the local networks connected through the Internet, the network IDs are divided into several classes, the most important of which are called *A*, *B*, and *C*. In every class, a host ID may not consist of either all 0's or all 1's.

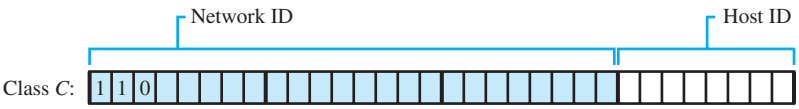
Class *A* network IDs are used for very large local networks. The left-most bit is set to 0, and the left-most 8 bits give the full network ID. The remaining 24 bits are used for individual host IDs. However, neither 00000000 nor 01111111 is allowed as a network ID for a class *A* IP address.



Class *B* network IDs are used for medium to large local networks. The two left-most bits are set to 10, and the left-most 16 bits give the full network ID. The remaining 16 bits are used for individual host IDs.



Class *C* network IDs are used for small local networks. The three left-most bits are set to 110, and the left-most 24 bits give the full network ID. The remaining 8 bits are used for individual host IDs.



a. Check that the dotted decimal form of 10001100 11000000 00100000 10001000 is 140.192.32.136.

b. How many Class *B* networks can there be?

c. What is the dotted decimal form of the IP address for a computer in a Class *B* network?

d. How many host IDs can there be for a Class *B* network?

Solution

a. $10001100 = 1\cdot 2^7 + 1\cdot 2^3 + 1\cdot 2^2 = 128 + 8 + 4 = 140$
$11000000 = 1\cdot 2^7 + 1\cdot 2^6 = 128 + 64 = 192$
$00100000 = 1\cdot 2^5 = 32$
$10001000 = 1\cdot 2^7 + 1\cdot 2^3 = 128 + 8 = 136$

b. The network ID for a Class *B* network consists of 16 bits and begins with 10. Because there are two choices for each of the remaining 14 positions (either 0 or 1), the total number of possible network IDs is 2^{14}, or 16,384.

c. The network ID part of a Class *B* IP address goes from

$$10000000\ 00000000 \quad \text{to} \quad 10111111\ 11111111.$$

As dotted decimals, these numbers range from 128.0 to 191.255 because $10000000_2 = 128_{10}$, $00000000_2 = 0_{10}$, $10111111_2 = 191_{10}$, $11111111_2 = 255_{10}$. Thus the dotted decimal form of the IP address of a computer in a Class *B* network is *w.x.y.z*, where $128 \le w \le 191$, $0 \le x \le 255$, $0 \le y \le 255$, and $0 \le z \le 255$. However, *y* and *z* are not allowed both to be 0 or both to be 255 because host IDs may not consist of either all 0's or all 1's.

d. For a class *B* network, 16 bits are used for host IDs. Having two choices (either 0 or 1) for each of 16 positions gives a potential total of 2^{16}, or 65,536, host IDs. But because two of these are not allowed (all 0's and all 1's), the total number of host IDs is 65,534. ■

The Inclusion/Exclusion Rule

The addition rule says how many elements are in a union of sets if the sets are mutually disjoint. Now consider the question of how to determine the number of elements in a union of sets when some of the sets overlap. For simplicity, begin by looking at a union of two sets *A* and *B*, as shown in Figure 9.3.5.

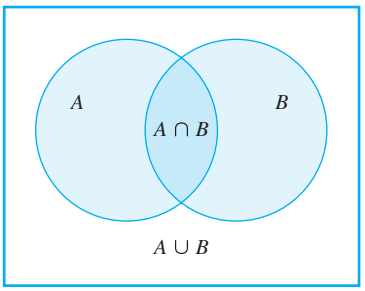


FIGURE 9.3.5

First observe that the number of elements in $A \cup B$ varies according to the number of elements the two sets have in common. If A and B have no elements in common, then $N(A \cup B) = N(A) + N(B)$. If A and B coincide, then $N(A \cup B) = N(A)$. Thus any general formula for $N(A \cup B)$ must contain a reference to the number of elements the two sets have in common, $N(A \cap B)$, as well as to $N(A)$ and $N(B)$.

The simplest way to derive a formula for $N(A \cup B)$ is to reason as follows: The number $N(A)$ counts the elements that are in A and not in B as well as the elements that are in both A and B. Similarly, the number $N(B)$ counts the elements that are in B and not in A as well as the elements that are in both A and B. Hence when the two numbers $N(A)$ and $N(B)$ are added, the elements that are in both A and B are counted twice. To get an accurate count of the elements in $A \cup B$, it is necessary to subtract the number of elements that are in both A and B. Because these are exactly the elements that are in $A \cap B$,

$$N(A \cup B) = N(A) + N(B) - N(A \cap B).$$

Note An alternative proof is outlined in exercise 46 at the end of this section.

A similar analysis gives a formula for the number of elements in a union of three sets, as shown in Theorem 9.3.3.

Theorem 9.3.3 The Inclusion/Exclusion Rule for Two or Three Sets

If A, B, and C are any finite sets, then

$$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

and

$$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C).$$

It can be shown using mathematical induction (see exercise 48 at the end of this section) that formulas analogous to those of Theorem 9.3.3 hold for unions of any finite number of sets.

Example 9.3.6 **Counting Elements of a General Union**

a. How many integers from 1 through 1,000 are multiples of 3 or multiples of 5?

b. How many integers from 1 through 1,000 are neither multiples of 3 nor multiples of 5?

Solution

a. Let A = the set of all integers from 1 through 1,000 that are multiples of 3.
Let B = the set of all integers from 1 through 1,000 that are multiples of 5.

Then

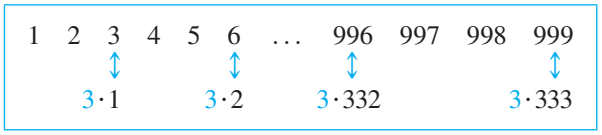
$A \cup B$ = the set of all integers from 1 through 1,000 that are multiples of 3 or multiples of 5

and

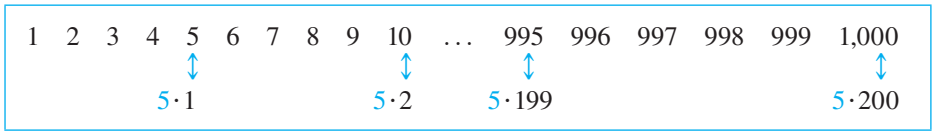
$A \cap B$ = the set of all integers from 1 through 1,000 that are multiples of both 3 and 5
= the set of all integers from 1 through 1,000 that are multiples of 15.

[Now calculate $N(A)$, $N(B)$, and $N(A \cap B)$ and use the inclusion/exclusion rule to solve for $N(A \cup B)$.]

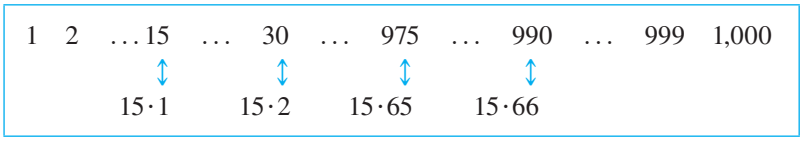
Because every third integer from 3 through 999 is a multiple of 3, each can be represented in the form $3k$, for some integer k from 1 through 333. Hence there are 333 multiples of 3 from 1 through 1,000, and so $N(A) = 333$.



Similarly, each multiple of 5 from 1 through 1,000 has the form $5k$, for some integer k from 1 through 200.



Thus there are 200 multiples of 5 from 1 through 1,000 and $N(B) = 200$. Finally, each multiple of 15 from 1 through 1,000 has the form $15k$, for some integer k from 1 through 66 (since $990 = 66 \cdot 15$).



Hence there are 66 multiples of 15 from 1 through 1,000, and $N(A \cap B) = 66$. It follows by the inclusion/exclusion rule that

$$\begin{aligned} N(A \cup B) &= N(A) + N(B) - N(A \cap B) \\ &= 333 + 200 - 66 \\ &= 467. \end{aligned}$$

Thus, 467 integers from 1 through 1,000 are multiples of 3 or multiples of 5.

b. There are 1,000 integers from 1 through 1,000, and by part (a), 467 of these are multiples of 3 or multiples of 5. Thus, by the set difference rule, there are $1{,}000 - 467 = 533$ that are neither multiples of 3 nor multiples of 5. ■

Note that the solution to part (b) of Example 9.3.6 hid a use of De Morgan's law. The number of elements that are neither in A nor in B is $N(A^c \cap B^c)$, and by De Morgan's law, $A^c \cap B^c = (A \cup B)^c$. So $N((A \cup B)^c)$ was calculated using the set difference rule: $N((A \cup B)^c) = N(U) - N(A \cup B)$, where the universe U was the set of all integers from 1 through 1,000. Exercises 37–39 at the end of this section explore this technique further.

Example 9.3.7 **Counting the Number of Elements in an Intersection**

A professor in a discrete mathematics class passes out a form asking students to check all the mathematics and computer science courses they have recently taken. She found that, out of a total of 50 students in the class,

30 took precalculus;
18 took calculus;
26 took Python;
9 took both precalculus and calculus;
16 took both precalculus and Python;
8 took both calculus and Python;
47 took at least one of the three courses.

Note that when we write "30 students took precalculus," we mean that the total number of students who took precalculus is 30, and we allow for the possibility that some of these students may have taken one or both of the other courses. If we want to say that 30 students took precalculus *only* (and not either of the other courses), we will say so explicitly.

a. How many students did not take any of the three courses?

b. How many students took all three courses?

c. How many students took precalculus and calculus but not Python? How many students took precalculus but neither calculus nor Python?

Solution

a. By the difference rule, the number of students who did not take any of the three courses equals the number in the class minus the number who took at least one course. Thus the number of students who did not take any of the three courses is

$$50 - 47 = 3.$$

b. Let

$$P = \text{the set of students who took precalculus}$$
$$C = \text{the set of students who took calculus}$$
$$Y = \text{the set of students who took Python.}$$

Then, by the inclusion/exclusion rule,

$$N(P \cup C \cup Y) = N(P) + N(C) + N(Y) - N(P \cap C) - N(P \cap Y) - N(C \cap Y) + N(P \cap C \cap Y)$$

Substituting known values, we get

$$47 = 30 + 18 + 26 - 9 - 16 - 8 + N(P \cap C \cap Y).$$

Solving for $N(P \cap C \cap Y)$ gives

$$N(P \cap C \cap Y) = 6.$$

Hence there are six students who took all three courses. In general, if you know any seven of the eight terms in the inclusion/exclusion formula for three sets, you can solve for the eighth term.

c. To answer the questions of part (c), look at the diagram in Figure 9.3.6.

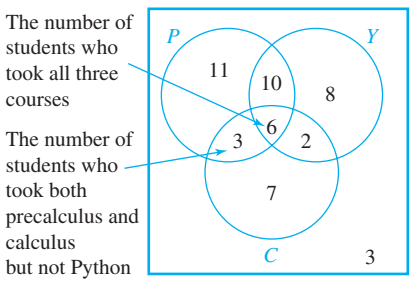


FIGURE 9.3.6

Since $N(P \cap C \cap Y) = 6$, put the number 6 inside the innermost region. Then work outward to find the numbers of students represented by the other regions of the diagram.

For example, since nine students took both precalculus and calculus and six took all three courses, $9 - 6 = 3$ students took precalculus and calculus but not Python. Similarly, since 16 students took precalculus and Python and six took all three courses, $16 - 6 = 10$ students took precalculus and Python but not calculus. Now the total number of students who took precalculus is 30. Of these 30, three also took calculus but not Python, ten took Python but not calculus, and six took both calculus and Python. That leaves 11 students who took precalculus but neither of the other two courses.

A similar analysis can be used to fill in the numbers for the other regions of the diagram. ■

TEST YOURSELF

1. The addition rule says that if a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots A_k$, then _____.
2. The difference rule says that if A is a finite set and B is a subset of A, then _____.
3. If S is a finite sample space and A is an event in S, then the probability of A^c equals _____.
4. The inclusion/exclusion rule for two sets says that if A and B are any finite sets, then _____.
5. The inclusion/exclusion rule for three sets says that if A, B, and C are any finite sets, then _____.

EXERCISE SET 9.3

1. **a.** How many bit strings consist of from one through four digits? (Strings of different lengths are considered distinct. Thus 10 and 0010 are distinct strings.)
   b. How many bit strings consist of from five through eight digits?
2. **a.** How many strings of hexadecimal digits consist of from one through three digits? (Recall that hexadecimal numbers are constructed using the 16 digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.)
   b. How many strings of hexadecimal digits consist of from two through five digits?
3. **a.** How many integers from 1 through 999 do not have any repeated digits?
   b. How many integers from 1 through 999 have at least one repeated digit?
   c. What is the probability that an integer chosen at random from 1 through 999 has at least one repeated digit?
4. How many arrangements in a row of no more than three letters can be formed using the letters of the word *NETWORK* (with no repetitions allowed)?
5. **a.** How many five-digit integers (integers from 10,000 through 99,999) are divisible by 5?
   b. What is the probability that a five-digit integer chosen at random is divisible by 5?
6. In a certain state, all license plates consist of from four to six symbols chosen from the 26 uppercase letters of the Roman alphabet together with the ten digits 0–9.
   a. How many license plates are possible if repetition of symbols is allowed?
   b. How many license plates do not contain any repeated symbols?
   c. How many license plates have at least one repeated symbol?
   d. What is the probability that a license plate chosen at random has at least one repeated symbol?
7. At a certain company, passwords must be from 3–5 symbols long and composed from the 26 uppercase letters of the Roman alphabet, the ten digits 0–9, and the 14 symbols !, @, #, $, %, ^, &, *, (,), −, +, {, and }.
   ***H* a.** How many passwords are possible if repetition of symbols is allowed?

b. How many passwords contain no repeated symbols?
c. How many passwords have at least one repeated symbol?
d. What is the probability that a password chosen at random has at least one repeated symbol?

8. In a certain country license plates consist of zero or one digit followed by four or five uppercase letters from the Roman alphabet.
a. How many different license plates can the country produce?
b. How many license plates have no repeated letter?
c. How many license plates have at least one repeated letter?
d. What is the probability that a license plate has a repeated letter?

9. a. Consider the following algorithm segment:

```
for i := 1 to 4
    for j := 1 to i
    [Statements in body of inner loop.
    None contain branching statements
    that lead outside the loop.]
    next j
next i
```

How many times will the inner loop be iterated when the algorithm is implemented and run?

b. Let n be a positive integer, and consider the following algorithm segment:

```
for i := 1 to n
    for j := 1 to i
    [Statements in body of inner loop.
    None contain branching statements
    that lead outside the loop.]
    next j
next i
```

How many times will the inner loop be iterated when the algorithm is implemented and run?

* **10.** A calculator has an eight-digit display and a decimal point that is located at the extreme right of the number displayed, or at the extreme left, or between any pair of digits. The calculator can also display a minus sign at the extreme left of the number. How many distinct numbers can the calculator display? (Note that certain numbers are equal, such as 1.9, 1.90, and 01.900, and should, therefore, not be counted twice.)

11. a. How many ways can the letters of the word *QUICK* be arranged in a row?
b. How many ways can the letters of the word *QUICK* be arranged in a row if the *Q* and the *U* must remain next to each other in the order *QU*?
c. How many ways can the letters of the word *QUICK* be arranged in a row if the letters *QU* must remain together but may be in either the order *QU* or the order *UQ*?

12. a. How many ways can the letters of the word *THEORY* be arranged in a row?
b. How many ways can the letters of the word *THEORY* be arranged in a row if *T* and *H* must remain next to each other as either *TH* or *HT*?

13. A group of eight people are attending the movies together.
a. Two of the eight insist on sitting side-by-side. In how many ways can the eight be seated together in a row?
b. Two of the people do not like each other and do not want to sit side-by-side. Now how many ways can the eight be seated together in a row?

14. An early compiler recognized variable names according to the following rules: Numeric variable names had to begin with a letter, and then the letter could be followed by another letter or a digit or by nothing at all. String variable names had to begin with the symbol $ followed by a letter, which could then be followed by another letter or a digit or by nothing at all. How many distinct variable names were recognized by this compiler?

H **15.** Identifiers in a certain database language must begin with a letter, and then the letter may be followed by other characters, which can be letters, digits, or underscores (_). However, 82 keywords (all consisting of 15 or fewer characters) are reserved and cannot be used as identifiers. How many identifiers with 30 or fewer characters are possible? (Write the answer using summation notation and evaluate it using a formula from Section 5.2.)

16. a. If any seven digits could be used to form a telephone number, how many seven-digit telephone numbers would not have any repeated digits?

b. How many seven-digit telephone numbers would have at least one repeated digit?
c. What is the probability that a randomly chosen seven-digit telephone number would have at least one repeated digit?

17. a. How many strings of four hexadecimal digits do not have any repeated digits?
b. How many strings of four hexadecimal digits have at least one repeated digit?
c. What is the probability that a randomly chosen string of four hexadecimal digits has at least one repeated digit?

18. Just as the difference rule gives rise to a formula for the probability of the complement of an event, so the addition and inclusion/exclusion rules give rise to formulas for the probability of the union of mutually disjoint events and for a general union of (not necessarily mutually exclusive) events.
a. Prove that for mutually disjoint events A and B,
$$P(A \cup B) = P(A) + P(B).$$
b. Prove that for any events A and B,
$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

H 19. A combination lock requires three selections of numbers, each from 1 through 39. Suppose the lock is constructed in such a way that no number may be used twice in a row but the same number may occur both first and third. For example, 20 13 20 would be acceptable, but 20 20 13 would not. How many different combinations are possible?

*** 20. a.** How many integers from 1 through 100,000 contain the digit 6 exactly once?
b. How many integers from 1 through 100,000 contain the digit 6 at least once?
c. If an integer is chosen at random from 1 through 100,000, what is the probability that it contains two or more occurrences of the digit 6?

H* 21. Six new employees, two of whom are married to each other, are to be assigned six desks that are lined up in a row. If the assignment of employees to desks is made randomly, what is the probability that the married couple will have nonadjacent desks? (*Hint:* The event that the couple have nonadjacent desks is the complement of the event that they have adjacent desks.)

*** 22.** Consider strings of length n over the set $\{a, b, c, d\}$.
a. How many such strings contain at least one pair of adjacent characters that are the same?
b. If a string of length ten over $\{a, b, c, d\}$ is chosen at random, what is the probability that it contains at least one pair of adjacent characters that are the same?

23. a. How many integers from 1 through 1,000 are multiples of 4 or multiples of 7?
b. Suppose an integer from 1 through 1,000 is chosen at random. Use the result of part (a) to find the probability that the integer is a multiple of 4 or a multiple of 7.
c. How many integers from 1 through 1,000 are neither multiples of 4 nor multiples of 7?

24. a. How many integers from 1 through 1,000 are multiples of 2 or multiples of 9?
b. Suppose an integer from 1 through 1,000 is chosen at random. Use the result of part (a) to find the probability that the integer is a multiple of 2 or a multiple of 9.
c. How many integers from 1 through 1,000 are neither multiples of 2 nor multiples of 9?

25. *Counting Strings:*
a. Make a list of all bit strings of lengths 0, 1, 2, 3, and 4 that do not contain the bit pattern 111.
b. For each integer $n \geq 0$, let d_n = the number of bit strings of length n that do not contain the bit pattern 111. Find d_0, d_1, d_2, d_3, and d_4.
c. Find a recurrence relation for $d_0, d_1, d_2, \ldots$.
d. Use the results of parts (b) and (c) to find the number of bit strings of length 5 that do not contain the pattern 111.

26. *Counting Strings:* Consider the set of all strings of a's, b's, and c's.
a. Make a list of all of these strings of lengths 0, 1, 2, and 3 that do not contain the pattern aa.
b. For each integer $n \geq 0$, let s_n = the number of strings of a's, b's, and c's of length n that do not contain the pattern aa. Find s_0, s_1, s_2, and s_3.
H c. Find a recurrence relation for $s_0, s_1, s_2, \ldots$.
d. Use the results of parts (b) and (c) to find the number of strings of a's, b's, and c's of length four that do not contain the pattern aa.
H e. Use the technique described in Section 5.8 to find an explicit formula for $s_0, s_1, s_2, \ldots$.

27. For each integer $n \geq 0$, let a_k be the number of bit strings of length n that do not contain the pattern 101.
a. Show that $a_k = a_{k-1} + a_{k-3} + a_{k-4} + \cdots + a_0 + 2$, for every integer $k \geq 3$.
b. Use the result of part (a) to show that if $k \geq 3$, then $a_k = 2a_{k-1} - a_{k-2} + a_{k-3}$.

* **28.** For each integer $n \geq 2$ let a_n be the number of permutations of $\{1, 2, 3, \ldots, n\}$ in which no number is more than one place removed from its "natural" position. Thus $a_1 = 1$ since the one permutation of $\{1\}$, namely, 1, does not move 1 from its natural position. Also, $a_2 = 2$ since neither of the two permutations of $\{1, 2\}$, namely, 12 and 21, moves either number more than one place from its natural position.
  - **a.** Find a_3.
  - **b.** Find a recurrence relation for $a_1, a_2, a_3, \ldots$.

29. Refer to Example 9.3.5.
  - **a.** Write the following IP address in dotted decimal form:

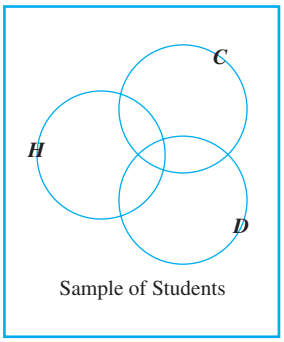
    11001010 00111000 01101011 11101110
  - **b.** How many Class *A* networks can there be?
  - **c.** What is the dotted decimal form of the IP address for a computer in a Class *A* network?
  - **d.** How many host IDs can there be for a Class *A* network?
  - **e.** How many Class *C* networks can there be?
  - **f.** What is the dotted decimal form of the IP address for a computer in a Class *C* network?
  - **g.** How many host IDs can there be for a Class *C* network?
  - **h.** How can you tell, by looking at the first of the four numbers in the dotted decimal form of an IP address, what kind of network the address is from? Explain.
  - **i.** An IP address is 140.192.32.136. What class of network does it come from?
  - **j.** An IP address is 202.56.107.238. What class of network does it come from?

* **30.** A row in a classroom has n seats. Let s_n be the number of ways nonempty sets of students can sit in the row so that no student is seated directly adjacent to any other student. (For instance, a row of three seats could contain a single student in any of the seats or a pair of students in the two outer seats. Thus $s_3 = 4$.) Find a recurrence relation for $s_1, s_2, s_3, \ldots$.

31. Assume that birthdays are equally likely to occur in any one of the 12 months of the year.
  - **a.** Given a group of four people, *A*, *B*, *C*, and *D*, what is the total number of ways in which birth months could be associated with *A*, *B*, *C*, and *D*? (For instance, *A* and *B* might have been born in May, *C* in September, and *D* in February. As another example, *A* might have been born in January, *B* in June, *C* in March, and *D* in October.)
  - **b.** How many ways could birth months be associated with *A*, *B*, *C*, and *D* so that no two people would share the same birth month?
  - **c.** How many ways could birth months be associated with *A*, *B*, *C*, and *D* so that at least two people would share the same birth month?
  - **d.** What is the probability that at least two people out of *A*, *B*, *C*, and *D* share the same birth month?
  - **e.** How large must n be so that in any group of n people, the probability that two or more share the same birth month is at least 50%?

H **32.** Assuming that all years have 365 days and all birthdays occur with equal probability, how large must n be so that in any randomly chosen group of n people, the probability that two or more have the same birthday is at least 1/2? (This is called the **birthday problem**. Many people find the answer surprising.)

33. A college conducted a survey to explore the academic interests and achievements of its students. It asked students to place checks beside the numbers of all the statements that were true of them. Statement #1 was "I was on the Dean's list last term," statement #2 was "I belong to an academic club, such as the math club or the Spanish club," and statement #3 was "I am majoring in at least two subjects." Out of a sample of 100 students, 28 checked #1, 26 checked #2, and 14 checked #3, 8 checked both #1 and #2, 4 checked both #1 and #3, 3 checked both #2 and #3, and 2 checked all three statements.
  - **a.** How many students checked at least one of the statements?
  - **b.** How many students checked none of the statements?
  - **c.** Let *H* be the set of students who checked #1, *C* the set of students who checked #2, and *D* the set of students who checked #3. Fill in the numbers for all eight regions of the diagram.



d. How many students checked #1 and #2 but not #3?

e. How many students checked #2 and #3 but not #1?

f. How many students checked #2 but neither of the other two?

34. A study was done to determine the efficacy of three different drugs—*A*, *B*, and *C*—in relieving headache pain. Over the period covered by the study, 50 subjects were given the chance to use all three drugs. The following results were obtained:

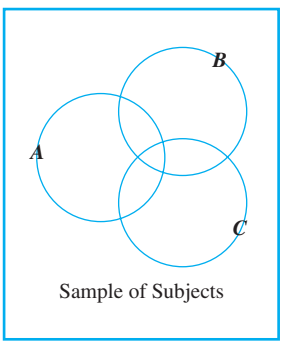
21 reported relief from drug *A*
21 reported relief from drug *B*
31 reported relief from drug *C*
9 reported relief from both drugs *A* and *B*
14 reported relief from both drugs *A* and *C*
15 reported relief from both drugs *B* and *C*
41 reported relief from at least one of the drugs.

Note that some of the 21 subjects who reported relief from drug *A* may also have reported relief from drugs *B* or *C*. A similar occurrence may be true for the other data.

a. How many people got relief from none of the drugs?

b. How many people got relief from all three drugs?

c. Let *A* be the set of all subjects who got relief from drug *A*, *B* the set of all subjects who got relief from drug *B*, and *C* the set of all subjects who got relief from drug *C*. Fill in the numbers for all eight regions of the following diagram.



d. How many subjects got relief from *A* only?

35. An interesting use of the inclusion/exclusion rule is to check survey numbers for consistency. For example, suppose a public opinion polltaker reports that out of a national sample of 1,200 adults, 675 are married, 682 are from 20 to 30 years old, 684 are female, 195 are married and are from 20 to 30 years old, 467 are married females, 318 are females from 20 to 30 years old, and 165 are married females from 20 to 30 years old. Are the polltaker's figures consistent? Could they have occurred as a result of an actual sample survey?

36. Fill in the reasons for each step below. If *A* and *B* are sets in a finite universe *U*, then

$$N(A \cap B) = N(U) - N((A \cap B)^c) \quad \underline{\text{(a)}}$$
$$= N(U) - N(A^c \cup B^c) \quad \underline{\text{(b)}}$$
$$= N(U) - (N(A^c) + N(B^c) - N(A^c \cap B^c)) \quad \underline{\text{(c)}}.$$

For each of exercises 37–39, the number of elements in a certain set can be found by computing the number in a larger universe that are not in the set and subtracting this from the total in the larger universe. In each of these, as was the case for the solution to Example 9.3.6(b), De Morgan's laws and the inclusion/exclusion rule can be used.

37. How many positive integers less than 1,000 have no common factors with 1,000?

* **38.** How many permutations of *abcde* are there in which the first character is *a*, *b*, or *c* and the last character is *c*, *d*, or *e*?

* **39.** How many integers from 1 through 999,999 contain each of the digits 1, 2, and 3 at least once? (*Hint:* For each $i = 1$, 2, and 3, let A_i be the set of all integers from 1 through 999,999 that do not contain the digit *i*.)

For 40 and 41, use the definition of the Euler phi function φ from Section 7.1, exercises 51–53.

H **40.** Use the inclusion/exclusion principle to prove the following: If $n = pq$, where p and q are distinct prime numbers, then $\varphi(n) = (p-1)(q-1)$.

41. Use the inclusion/exclusion principle to prove the following: If $n = pqr$, where p, q, and r are distinct prime numbers, then $\varphi(n) = (p-1)(q-1)(r-1)$.

42. A gambler decides to play successive games of blackjack until he loses three times in a row. (Thus the gambler could play five games by losing the first, winning the second, and losing the final three or by winning the first two and losing the final three. These possibilities can be symbolized as *LWLLL* and *WWLLL*.) Let g_n be the number of ways the gambler can play *n* games.

a. Find g_3, g_4, and g_5.

b. Find g_6.

H **c.** Find a recurrence relation for $g_3, g_4, g_5, \ldots$.

* **43.** A *derangement* of the set $\{1, 2, \ldots, n\}$ is a permutation that moves every element of the set away from its "natural" position. Thus 21 is a derangement of $\{1, 2\}$, and 231 and 312 are derangements of $\{1, 2, 3\}$. For each positive integer n, let d_n be the number of derangements of the set $\{1, 2, \ldots, n\}$.
   a. Find d_1, d_2, and d_3.
   b. Find d_4.
   H **c.** Find a recurrence relation for $d_1, d_2, d_3, \ldots$.

44. Note that a product $x_1x_2x_3$ may be parenthesized in two different ways: $(x_1x_2)x_3$ and $x_1(x_2x_3)$. Similarly, there are several different ways to parenthesize $x_1x_2x_3x_4$. Two such ways are $(x_1x_2)(x_3x_4)$ and $x_1((x_2x_3)x_4)$. Let P_n be the number of different ways to parenthesize the product $x_1x_2 \ldots x_4$. Show that if $P_1 = 1$, then

$$P_n = \sum_{k=1}^{n-1} P_k P_{n-k} \quad \text{for every integer } n \geq 2.$$

(It turns out that the sequence $P_1, P_2, P_3, \ldots$ is the same as the sequence of Catalan numbers: $P_n = C_{n-1}$ for every integer $n \geq 1$. See Example 5.6.4.)

45. Use mathematical induction to prove Theorem 9.3.1.

46. Prove the inclusion/exclusion rule for two sets A and B by showing that $A \cup B$ can be partitioned into $A \cap B$, $A - (A \cap B)$, and $B - (A \cap B)$, and then using the addition and difference rules. (See the hint for exercise 39 in Section 6.2.)

47. Prove the inclusion/exclusion rule for three sets.

H* **48.** Use mathematical induction to prove the general inclusion/exclusion rule:

If $A_1, A_2, \ldots, A_n$ are finite sets, then

$$N(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{1 \leq i \leq n} N(A_i) - \sum_{1 \leq i < j \leq n} N(A_i \cap A_j) + \sum_{1 \leq i < j < k \leq n} N(A_i \cap A_j \cap A_k) - \cdots + (-1)^{n+1} N(A_1 \cap A_2 \cap \cdots \cap A_n).$$

(The notation $\sum_{1 \leq i < j \leq n} N(A_i \cap A_j)$ means that quantities of the form $N(A_i \cap A_j)$ are to be added together for all integers i and j with $1 \leq i < j \leq n$.)

* **49.** A circular disk is cut into n distinct sectors, each shaped like a piece of pie and all meeting at the center point of the disk. Each sector is to be painted red, green, yellow, or blue in such a way that no two adjacent sectors are painted the same color. Let S_n be the number of ways to paint the disk.
   a. Find a recurrence relation for S_k in terms of S_{k-1} and S_{k-2} for each integer $k \geq 4$.
   b. Find an explicit formula for S_n for $n \geq 2$.

ANSWERS FOR TEST YOURSELF

1. the number of elements in A equals $N(A_1) + N(A_2) + \cdots + N(A_n)$ **2.** the number of elements in $A - B$ is the difference between the number of elements in A and the number of elements in B, that is, $N(A - B) = N(A) - N(B)$. **3.** $1 - P(A)$ **4.** $N(A \cup B) = N(A) + N(B) - N(A \cap B)$ **5.** $N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$

9.4 The Pigeonhole Principle

The shrewd guess, the fertile hypothesis, the courageous leap to a tentative conclusion—these are the most valuable coin of the thinker at work.
—Jerome S. Bruner, 1960

The pigeonhole principle states that if n pigeons fly into m pigeonholes and $n > m$, then at least one hole must contain two or more pigeons. This principle is illustrated in Figure 9.4.1 for $n = 5$ and $m = 4$. Illustration (a) shows the pigeons perched next to their holes, and (b) shows the correspondence from pigeons to pigeonholes. The pigeonhole principle is sometimes called the *Dirichlet box principle* because it was first stated formally by J. P. G. L. Dirichlet (1805–1859).

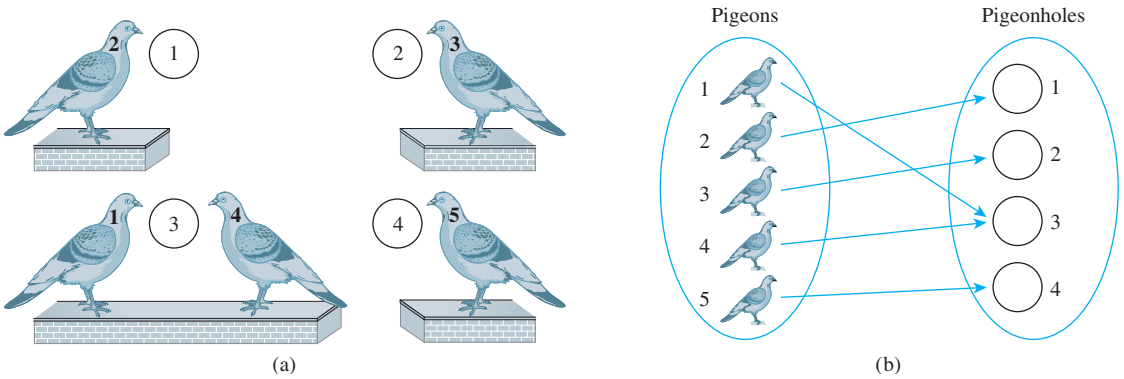


FIGURE 9.4.1

Illustration (b) suggests the following mathematical way to phrase the principle.

Pigeonhole Principle

A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least two elements in the domain that have the same image in the co-domain.

Thus an arrow diagram for a function from a finite set to a smaller finite set must have at least two arrows from the domain that point to the same element of the co-domain. In Figure 9.4.1(b), arrows from pigeons 1 and 4 both point to pigeonhole 3.

Since the truth of the pigeonhole principle is easy to accept intuitively, we move immediately to applications, leaving a formal proof to the end of the section. Applications of the pigeonhole principle range from the totally obvious to the extremely subtle. A representative sample is given in the examples and exercises that follow.

Example 9.4.1 **Applying the Pigeonhole Principle**

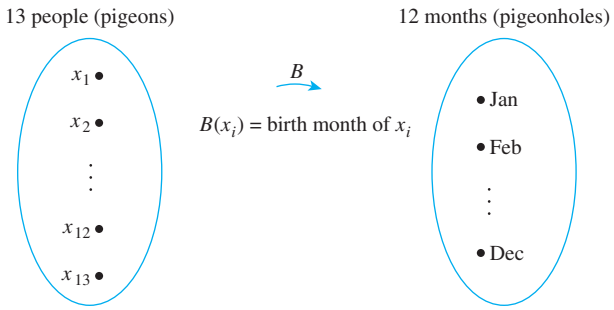
a. In a group of six people, must there be at least two who were born in the same month? In a group of thirteen people, must there be at least two who were born in the same month? Why?

b. Among the residents of New York City, must there be at least two people with the same number of hairs on their heads? Why?

Solution

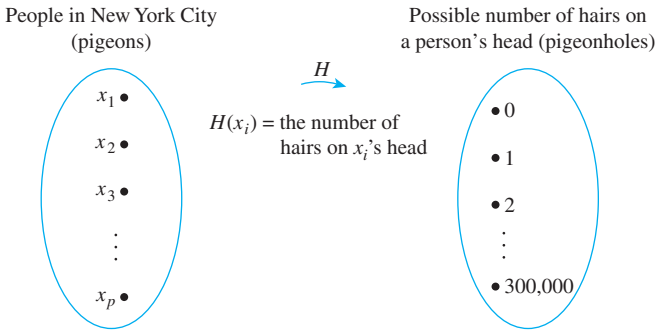
a. A group of six people need not contain two who were born in the same month. For instance, the six people could have birthdays in each of the six months January through June.

A group of 13 people, however, must contain at least two who were born in the same month, for there are only 12 months in a year and $13 > 12$. To get at the essence of this reasoning, think of the thirteen people as the pigeons and the twelve months of the year as the pigeonholes. Denote the thirteen people by the symbols $x_1, x_2, \ldots, x_{13}$ and define a function B from the set of people to the set of twelve months as shown in the following arrow diagram.



The pigeonhole principle says that no matter what the particular assignment of months to people, there must be at least two arrows pointing to the same month. Thus at least two people must have been born in the same month.

b. The answer is yes. In this example the pigeons are the people of New York City and the pigeonholes are all possible numbers of hairs on any individual's head. Call the population of New York City P. It is known that P is at least 8,000,000. Also, the maximum number of hairs on any person's head is known to be less than 300,000. Define a function H from the set of people in New York City $\{x_1, x_2, \ldots, x_p\}$ to the set $\{0, 1, 2, 3, \ldots, 300{,}000\}$, as shown in the arrow diagram.



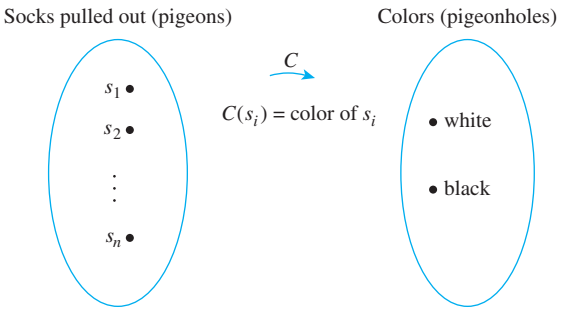
Since the number of people in New York City is larger than the number of possible hairs on their heads, the function H is not one-to-one; at least two arrows point to the same number. And this means that at least two people have the same number of hairs on their heads. ■

Example 9.4.2 **Finding the Number to Pick to Ensure a Result**

A drawer contains ten black and ten white socks. You reach in and pull some out without looking at them. What is the *least* number of socks you must pull out to be sure to get a matched pair? Explain how the answer follows from the pigeonhole principle.

Solution If you pick just two socks, they may have different colors. But when you pick a third sock, it must be the same color as one of the socks already chosen. Hence the answer is three.

This answer could be phrased more formally as follows: Let the socks pulled out be denoted $s_1, s_2, s_3, \ldots, s_n$ and consider the function C that sends each sock to its color, as shown on the next page.



If $n = 2$, C could be a one-to-one correspondence (if the two socks pulled out were of different colors). But if $n > 2$, then the number of elements in the domain of C is larger than the number of elements in the co-domain of C. Thus by the pigeonhole principle, C is not one-to-one: $C(s_i) = C(s_j)$ for some $s_i \neq s_j$. This means that if at least three socks are pulled out, then at least two of them have the same color. ■

Example 9.4.3 **Selecting a Pair of Integers with a Certain Sum**

Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

a. If five integers are selected from A, must at least one pair of the integers have a sum of 9?

b. If four integers are selected from A, must at least one pair of the integers have a sum of 9?

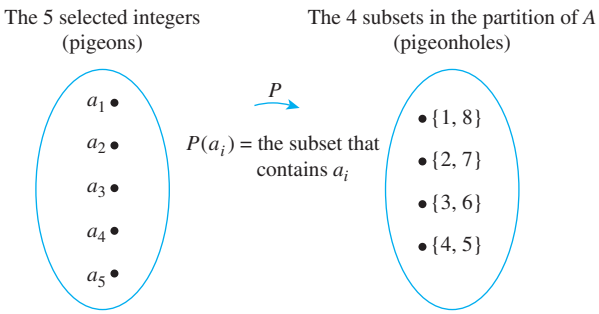
Solution

a. Yes. Partition the set A into the following four disjoint subsets:

$$\{1, 8\}, \quad \{2, 7\}, \quad \{3, 6\}, \quad \text{and} \quad \{4, 5\}.$$

Observe that each of the integers in A occurs in exactly one of the four subsets and that the sum of the integers in each subset is 9. Thus if five integers from A are chosen, then by the pigeonhole principle, two must be from the same subset. It follows that the sum of these two integers is 9.

To see precisely how the pigeonhole principle applies, let the pigeons be the five selected integers (call them a_1, a_2, a_3, a_4, and a_5) and let the pigeonholes be the subsets of the partition. The function P from pigeons to pigeonholes is defined by letting $P(a_i)$ be the subset that contains a_i.



The function P is well defined because for each integer a_i in the domain, a_i belongs to one of the subsets (since the union of the subsets is A) and a_i does not belong to more than one subset (since the subsets are disjoint).

Because there are more pigeons than pigeonholes, at least two pigeons must go to the same hole. Thus two distinct integers are sent to the same set. But that implies that those two integers are the two distinct elements of the set, so their sum is 9. More formally, by the pigeonhole principle, since P is not one-to-one, there are integers a_i and a_j such that

$$P(a_i) = P(a_j) \quad \text{and} \quad a_i \neq a_j.$$

But then, by definition of P, a_i and a_j belong to the same subset. Since the elements in each subset add up to 9, $a_i + a_j = 9$.

b. The answer is no. This is a case where the pigeonhole principle does not apply; the number of pigeons is not larger than the number of pigeonholes. For instance, if you select the integers 1, 2, 3, and 4, then since the largest sum of any two of these integers is 7, no two of them add up to 9. ■

Application to Decimal Expansions of Fractions

One important consequence of the pigeonhole principle is the fact that

the decimal expansion of any rational number either terminates or repeats.

A terminating decimal is one like

$$3.625,$$

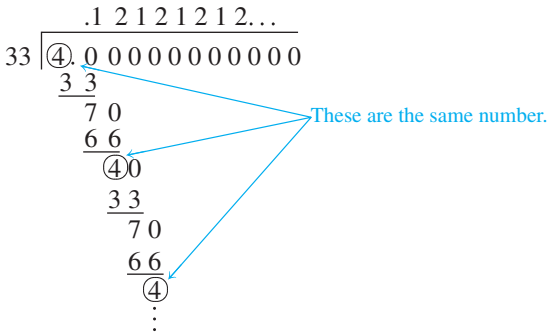
and a repeating decimal is one like

$$2.38\overline{246},$$

where the bar over the digits 246 means that these digits are repeated forever.

Note Strictly speaking, a terminating decimal like 3.625 can be regarded as a repeating decimal by adding trailing zeros: $3.625 = 3.625\overline{0}$. This can also be written as $3.624\overline{9}$.

Recall that a rational number is one that can be written as a ratio of integers—in other words, as a fraction. Recall also that the decimal expansion of a fraction is obtained by dividing its numerator by its denominator using long division. For example, the decimal expansion of $4/33$ is obtained as follows:

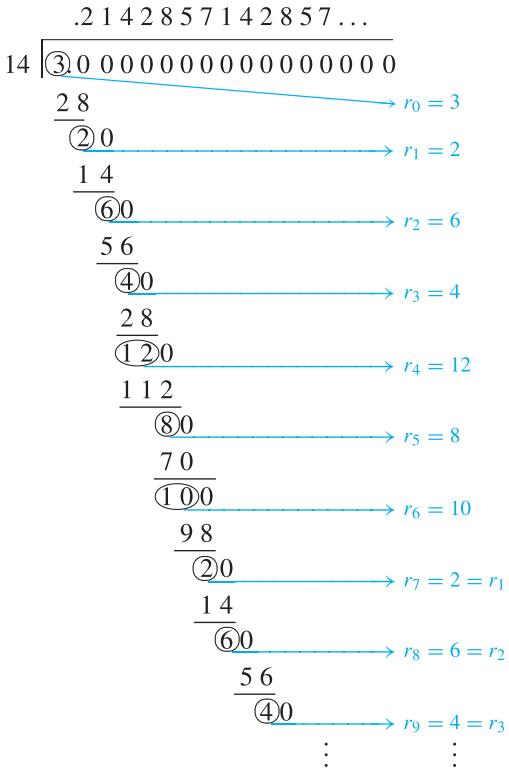


Because the number 4 reappears as a remainder in the long-division process, the sequence of quotients and remainders that give the digits of the decimal expansion repeats forever; hence the digits of the decimal expansion repeat forever.

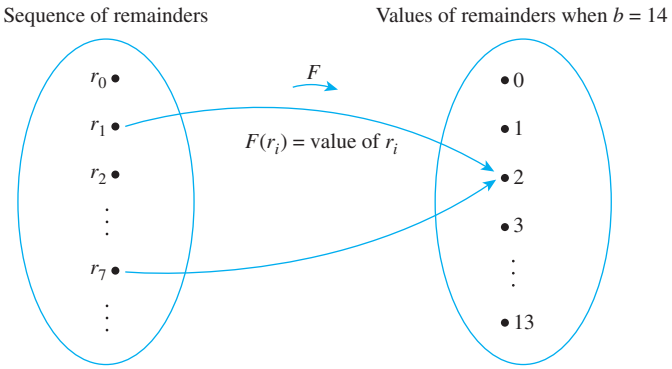
In general, when one integer is divided by another, it is the pigeonhole principle (together with the quotient-remainder theorem) that guarantees that such a repetition of remainders and hence decimal digits must always occur. This is explained in the following example. The analysis in the example uses an obvious generalization of the pigeonhole principle, namely, that a function from an infinite set to a finite set cannot be one-to-one.

Example 9.4.4 **The Decimal Expansion of a Fraction**

Let a and b be integers and consider a fraction a/b, where for simplicity a and b are both assumed to be positive. The decimal expansion of a/b is obtained by dividing a by b as illustrated here for $a = 3$ and $b = 14$.



Let $r_0 = a$ and let $r_1, r_2, r_3, \ldots$ be the successive remainders obtained in the long division of a by b. By the quotient-remainder theorem, each remainder must be between 0 and $b - 1$. (In this example, a is 3 and b is 14, and so the remainders are from 0 to 13.) If some remainder $r_i = 0$, then the division terminates and a/b has a terminating decimal expansion. If no $r_i = 0$, then the division process and hence the sequence of remainders continues forever. By the pigeonhole principle, since there are more remainders than values that the remainders can take, some remainder value must repeat: $r_j = r_k$, for some indices j and k with $j < k$. This is illustrated below for $a = 3$ and $b = 14$.



If follows that the decimal digits obtained from the divisions between r_j and r_{k-1} repeat forever. In the case of $3/14$, the repetition begins with $r_7 = 2 = r_i$ and the decimal expansion repeats the quotients obtained from the divisions from r_1 through r_6 forever: $3/14 = 0.2\overline{142857}$. ■

Note that since the decimal expansion of any rational number either terminates or repeats, if a number has a decimal expansion that neither terminates nor repeats, then it cannot be rational. Thus, for example, the following number cannot be rational: $0.01011011101111011111\ldots$ (where each string of 1's is one longer than the previous string).

Generalized Pigeonhole Principle

A generalization of the pigeonhole principle states that if n pigeons fly into m pigeonholes and, for some positive integer k, $km < n$, then at least one pigeonhole contains $k + 1$ or more pigeons. This is illustrated in Figure 9.4.2 for $m = 4$, $n = 9$, and $k = 2$. Since $2 \cdot 4 < 9$, at least one pigeonhole contains three $(2 + 1)$ or more pigeons. (In this example, pigeonhole 3 contains three pigeons.)

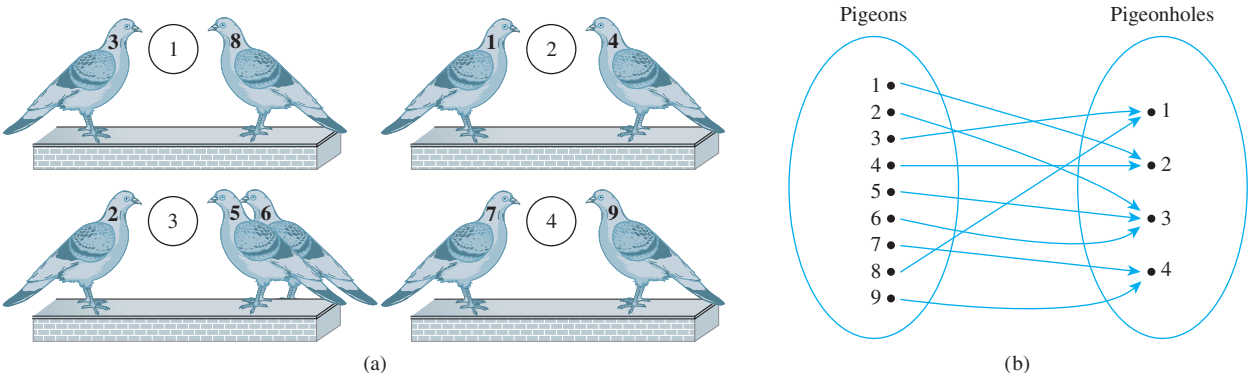


FIGURE 9.4.2

Generalized Pigeonhole Principle

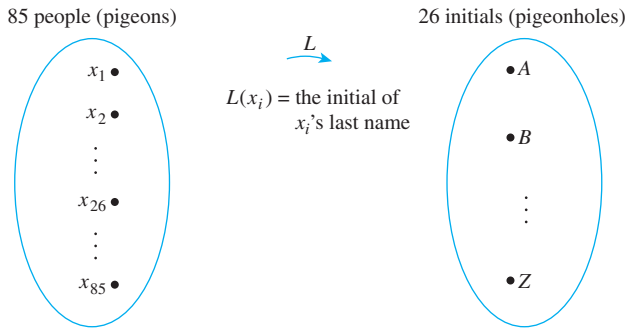
For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $km < n$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of X.

Example 9.4.5 **Applying the Generalized Pigeonhole Principle**

Show how the generalized pigeonhole principle implies that in a group of 85 people, at least 4 must have the same last initial.

Solution In this example the pigeons are the 85 people and the pigeonholes are the 26 possible last initials of their names.

Consider the function L from people to initials defined by the following arrow diagram.



Since $3 \cdot 26 = 78 < 85$, the generalized pigeonhole principle states that some initial must be the image of at least four $(3 + 1)$ people. Thus at least four people have the same last initial. ■

Consider the following contrapositive form of the generalized pigeonhole principle.

Generalized Pigeonhole Principle (Contrapositive Form)

For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(y)$ has at most k elements, then X has at most km elements; in other words, $n \leq km$.

You may find it natural to use the contrapositive form of the generalized pigeonhole principle in certain situations. For instance, the result of Example 9.4.5 can be explained as follows:

> Suppose no 4 people out of the 85 had the same last initial. Then at most 3 would share any particular one. By the generalized pigeonhole principle (contrapositive form), this would imply that the total number of people is at most $3 \cdot 26 = 78$. But this contradicts the fact that there are 85 people in all. Hence at least 4 people share a last initial.

Example 9.4.6 **Using the Contrapositive Form of the Generalized Pigeonhole Principle**

There are 42 students who are to share 12 computers. Each student uses exactly 1 computer, and no computer is used by more than 6 students. Show that at least 5 computers are used by 3 or more students.

Solution

a. ***Using an Argument by Contradiction:*** Suppose not. Suppose that 4 or fewer computers are used by 3 or more students. *[A contradiction will be derived.]* Then $12 - 4 = 8$ or more computers are used by 2 or fewer students. Divide the set of computers into two subsets: C_1 and C_2. Into C_1 place 8 of the computers used by 2 or fewer students;

into C_2 place the computers used by 3 or more students plus any remaining computers (to make a total of 4 computers in C_2). (See Figure 9.4.3.)

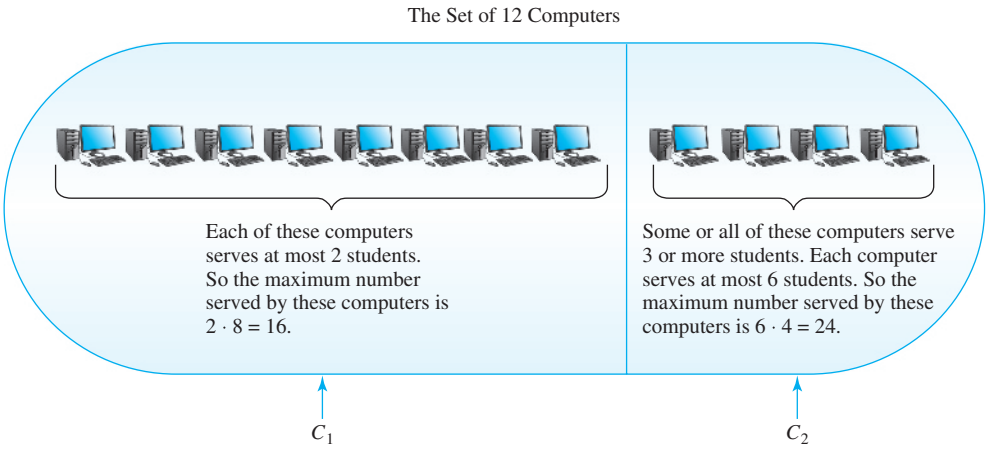


FIGURE 9.4.3

Since at most 6 students are served by any one computer, by the contrapositive form of the generalized pigeonhole principle, the computers in set C_2 serve at most $6 \cdot 4 = 24$ students. Since at most 2 students are served by any one computer in C_1, by the generalized pigeonhole principle (contrapositive form), the computers in set C_1 serve at most $2 \cdot 8 = 16$ students. Hence the total number of students served by the computers is $24 + 16 = 40$. But this contradicts the fact that each of the 42 students is served by a computer. Therefore, the supposition is false: At least 5 computers are used by 3 or more students.

b. ***Using a Direct Argument:*** Let k be the number of computers used by 3 or more students. *[We must show that $k \geq 5$.]* Because each computer is used by at most 6 students, these computers are used by at most $6k$ students (by the contrapositive form of the generalized pigeonhole principle). Each of the remaining $12 - k$ computers is used by at most 2 students. Hence, taken together, they are used by at most $2(12 - k) = 24 - 2k$ students (again, by the contrapositive form of the generalized pigeonhole principle). Thus the maximum number of students served by the computers is $6k + (24 - 2k) = 4k + 24$. Because 42 students are served by the computers, $4k + 24 \geq 42$. Solving for k gives that $k > 4.5$, and since k is an integer, this implies that $k \geq 5$ *[as was to be shown].* ■

Proof of the Pigeonhole Principle

The truth of the pigeonhole principle depends essentially on the sets involved being finite. Recall from Section 7.4 that a set is called **finite** if, and only if, it is the empty set or there is a one-to-one correspondence from $\{1, 2, \ldots, n\}$ to it, where n is a positive integer. In the first case the **number of elements** in the set is said to be 0, and in the second case it is said to be n. A set that is not finite is called **infinite**.

Thus any finite set is either empty or can be written in the form $\{x_1, x_2, \ldots, x_n\}$ where n is a positive integer.

Theorem 9.4.1 The Pigeonhole Principle

For any function f from a finite set X with n elements to a finite set Y with m elements, if $n > m$, then f is not one-to-one.

Proof: Suppose f is any function from a finite set X with n elements to a finite set Y with m elements where $n > m$. Denote the elements of Y by $y_1, y_2, \ldots, y_m$. Recall that for each y_i in Y, the inverse image set $f^{-1}(y_i) = \{x \in X \mid f(x) = y_i\}$. Now consider the collection of all the inverse image sets for all the elements of Y:

$$f^{-1}(y_1), f^{-1}(y_2), \ldots, f^{-1}(y_m).$$

By definition of function, each element of X is sent by f to some element of Y. Hence each element of X is in one of the inverse image sets, and so the union of all these sets equals X. But also, by definition of function, no element of X is sent by f to more than one element of Y. Thus each element of X is in only one of the inverse image sets, and so the inverse image sets are mutually disjoint. By the addition rule, therefore,

$$N(X) = N(f^{-1}(y_1)) + N(f^{-1}(y_2)) + \cdots + N(f^{-1}(y_m)). \qquad 9.4.1$$

Now suppose that f is one-to-one *[which is the opposite of what we want to prove]*. Then each set $f^{-1}(y_i)$ has at most one element, and so

$$N(f^{-1}(y_1)) + N(f^{-1}(y_2)) + \cdots + N(f^{-1}(y_m)) \leq \underbrace{1 + 1 + \cdots + 1}_{m \text{ terms}} = m \qquad 9.4.2$$

Putting equations (9.4.1) and (9.4.2) together gives that

$$n = N(X) \leq m = N(Y).$$

This contradicts the fact that $n > m$, and so the supposition that f is one-to-one must be false. Hence f is not one-to-one *[as was to be shown]*.

An important theorem that follows from the pigeonhole principle states that a function from one finite set to another finite set of the same size is one-to-one if, and only if, it is onto. As shown in Section 7.4, this result does not hold for infinite sets.

Theorem 9.4.2 One-to-One and Onto for Finite Sets

Let X and Y be finite sets with the same number of elements and suppose f is a function from X to Y. Then f is one-to-one if, and only if, f is onto.

Proof: Suppose f is a function from X to Y, where X and Y are finite sets each with m elements. Let $X = \{x_1, x_2, \ldots, x_m\}$ and $Y = \{y_1, y_2, \ldots, y_m\}$.

If f is one-to-one, then f is onto: Suppose f is one-to-one. Then $f(x_1), f(x_2), \ldots, f(x_m)$ are all distinct. Consider the set S of all elements of Y that are not the image of any element of X.

Then the sets

$$\{f(x_1)\}, \{f(x_2)\}, \ldots, \{f(x_m)\} \quad \text{and} \quad S$$

(continued on page 614)

are mutually disjoint. By the addition rule,

$$\begin{aligned} N(Y) &= N(\{f(x_1)\}) + N(\{f(x_2)\}) + \cdots + N(\{f(x_m)\}) + N(S) \\ &= \underbrace{1 + 1 + \cdots + 1}_{m \text{ terms}} + N(S) \qquad \text{because each } \{f(x_i)\} \text{ is a singleton set} \\ &= m + N(S). \end{aligned}$$

Thus

$$m = m + N(S) \qquad \text{because } N(Y) = m,$$

and so

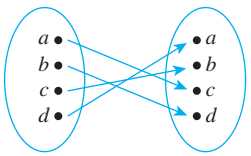
$$N(S) = 0 \qquad \text{by subtracting } m \text{ from both sides.}$$

Hence S is empty, and so there is no element of Y that is not the image of some element of X. Consequently, f is onto.

If f is onto, then f is one-to-one: Suppose f is onto. Then, for each $i = 1, 2, \ldots, m$, $f^{-1}(y_i) \neq \varnothing$ and so $N(f^{-1}(y_i)) \geq 1$. As in the proof of the pigeonhole principle (Theorem 9.4.1), X is the union of the mutually disjoint sets $f^{-1}(y_1), f^{-1}(y_2), \ldots, f^{-1}(y_m)$. By the addition principle,

$$N(X) = \underbrace{N(f^{-1}(y_1)) + N(f^{-1}(y_2)) + \cdots + N(f^{-1}(y_m))}_{m \text{ terms, each} \geq 1} \geq m \qquad 9.4.3$$

Now if any one of the sets $f^{-1}(y_i)$ has more than one element, then the sum of the m terms in equation (9.4.3) is greater than m. But we know this is not the case because $N(X) = m$. Hence each set $f^{-1}(y_i)$ has exactly one element, and thus f is one-to-one *[as was to be shown]*.



Note that Theorem 9.4.2 applies in particular to the case $X = Y$. Thus a one-to-one function from a finite set to itself is onto, and an onto function from a finite set to itself is one-to-one. Such functions are permutations of the sets on which they are defined. For instance, the function defined by the diagram on the left is another representation for the permutation *cdba* obtained by listing the images of a, b, c, and d in order.

TEST YOURSELF

1. The pigeonhole principle states that _____.
2. The generalized pigeonhole principle states that _____.
3. If X and Y are finite sets and f is a function from X to Y then f is one-to-one if, and only if, _____.

EXERCISE SET 9.4

1. **a.** If 4 cards are selected from a standard 52-card deck, must at least 2 be of the same suit? Why?
   b. If 5 cards are selected from a standard 52-card deck, must at least 2 be of the same suit? Why?

2. **a.** If 13 cards are selected from a standard 52-card deck, must at least 2 be of the same denomination? Why?
   b. If 20 cards are selected from a standard 52-card deck, must at least 2 be of the same denomination? Why?

3. A small town has only 500 residents. Must there be 2 residents who have the same birthday? Why?

4. In a group of 700 people, must there be 2 who have the same first and last initials? Why?

5. **a.** Given any set of four integers, must there be two that have the same remainder when divided by 3? Why?
   b. Given any set of three integers, must there be two that have the same remainder when divided by 3? Why?

6. **a.** Given any set of seven integers, must there be two that have the same remainder when divided by 6? Why?
   b. Given any set of seven integers, must there be two that have the same remainder when divided by 8? Why?

H 7. Let $S = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Suppose six integers are chosen from S. Must there be two integers whose sum is 15? Why?

8. Let $T = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Suppose five integers are chosen from T. Must there be two integers whose sum is 10? Why?

9. **a.** If seven integers are chosen from between 1 and 12 inclusive, must at least one of them be odd? Why?
   b. If ten integers are chosen from between 1 and 20 inclusive, must at least one of them be even? Why?

10. If $n + 1$ integers are chosen from the set

$$\{1, 2, 3, \ldots, 2n\},$$

where n is a positive integer, must at least one of them be odd? Why?

11. If $n + 1$ integers are chosen from the set

$$\{1, 2, 3, \ldots, 2n\},$$

where n is a positive integer, must at least one of them be even? Why?

12. How many cards must you pick from a standard 52-card deck to be sure of getting at least 1 red card? Why?

13. Suppose six pairs of similar-looking boots are thrown together in a pile. How many individual boots must you pick to be sure of getting a matched pair? Why?

14. How many integers from 0 through 60 must you pick in order to be sure of getting at least one that is odd? at least one that is even?

15. If n is a positive integer, how many integers from 0 through $2n$ must you pick in order to be sure of getting at least one that is odd? at least one that is even?

16. How many integers from 1 through 100 must you pick in order to be sure of getting one that is divisible by 5?

17. How many integers must you pick in order to be sure that at least two of them have the same remainder when divided by 7?

18. How many integers must you pick in order to be sure that at least two of them have the same remainder when divided by 15?

19. How many integers from 100 through 999 must you pick in order to be sure that at least two of them have a digit in common? (For example, 256 and 530 have the digit 5 in common.)

20. **a.** If repeated divisions by 20,483 are performed, how many distinct remainders can be obtained?
   b. When $5/20483$ is written as a decimal, what is the maximum length of the repeating section of the representation?

21. When $683/1493$ is written as a decimal, what is the maximum length of the repeating section of the representation?

22. Is 0.101001000100001000001 . . . (where each string of 0's is one longer than the previous one) rational or irrational?

23. Is 56.556655566655556666 . . . (where the strings of 5's and 6's become longer in each repetition) rational or irrational?

24. Show that within any set of thirteen integers chosen from 2 through 40, there are at least two integers with a common divisor greater than 1.

25. In a group of 30 people, must at least 3 have been born in the same month? Why?

26. In a group of 30 people, must at least 4 have been born in the same month? Why?

27. In a group of 2,000 people, must at least 5 have the same birthday? Why?

28. A programmer writes 500 lines of computer code in 17 days. Must there have been at least 1 day

when the programmer wrote 30 or more lines of code? Why?

29. A certain college class has 40 students. All the students in the class are known to be from 17 through 34 years of age. You want to make a bet that the class contains at least x students of the same age. How large can you make x and yet be sure to win your bet?

30. A penny collection contains twelve 1967 pennies, seven 1968 pennies, and eleven 1971 pennies. If you are to pick some pennies without looking at the dates, how many must you pick to be sure of getting at least five pennies from the same year?

***H* 31.** A group of 15 executives are to share 5 assistants. Each executive is assigned exactly 1 assistant, and no assistant is assigned to more than 4 executives. Show that at least 3 assistants are assigned to 3 or more executives.

***H**32.** Let A be a set of six positive integers each of which is less than 13. Show that there must be two distinct subsets of A whose elements when added up give the same sum. (For example, if $A = \{5, 12, 10, 1, 3, 4\}$, then the elements of the subsets $S_1 = \{1, 4, 10\}$ and $S_2 = \{5, 10\}$ both add up to 15.)

***H* 33.** Let A be a set of six positive integers each of which is less than 15. Show that there must be two distinct subsets of A whose elements when added up give the same sum. (Thanks to Jonathan Goldstine for this problem.)

34. Let S be a set of ten integers chosen from 1 through 50. Show that the set contains at least two different (but not necessarily disjoint) subsets of four integers that add up to the same number. (For instance, if the ten numbers are {3, 8, 9, 18, 24, 34, 35, 41, 44, 50}, the subsets can be taken to be {8, 24, 34, 35} and {9, 18, 24, 50}. The numbers in both of these add up to 101.)

***H**35.** Given a set of 52 distinct integers, show that there must be 2 whose sum or difference is divisible by 100.

***H**36.** Show that if 101 integers are chosen from 1 to 200 inclusive, there must be 2 with the property that one is divisible by the other.

*** 37. a.** Suppose $a_1, a_2, \ldots, a_n$ is a sequence of n integers none of which is divisible by n. Show that at least one of the differences $a_i - a_j$ (for $i \neq j$) must be divisible by n.

***H* b.** Show that every finite sequence $x_1, x_2, \ldots, x_n$ of n integers has a consecutive subsequence $x_{i+1}, x_{i+2}, \ldots, x_j$ whose sum is divisible by n. (For instance, the sequence 3, 4, 17, 7, 16 has the consecutive subsequence 17, 7, 16 whose sum is divisible by 5.) (From: James E. Schultz and William F. Burger, "An Approach to Problem-Solving Using Equivalence Classes Modulo n," *College Mathematics Journal* (15), No. 5, 1984, 401–405.)

***H**38.** Observe that the sequence 12, 15, 8, 13, 7, 18, 19, 11, 14, 10 has three increasing subsequences of length four: 12, 15, 18, 19; 12, 13, 18, 19; and 8, 13, 18, 19. It also has one decreasing subsequence of length four: 15, 13, 11, 10. Show that in any sequence of $n^2 + 1$ distinct real numbers, there must be a sequence of length $n + 1$ that is either strictly increasing or strictly decreasing.

*** 39.** What is the largest number of elements that a set of integers from 1 through 100 can have so that no one integer in the set is divisible by another? (*Hint*: Imagine writing all the integers from 1 through 100 in the form $2^k \cdot m$, where $k \geq 0$ and m is odd.)

40. Suppose X and Y are finite sets, X has more elements than Y, and F: $X \longrightarrow Y$ is a function. By the pigeonhole principle, there exist elements a and b in X such that $a \neq b$ and $F(a) = F(b)$. Write a computer algorithm to find such a pair of elements a and b.

ANSWERS FOR TEST YOURSELF

1. if n pigeons fly into m pigeonholes and $n > m$, then at least two pigeons fly into the same pigeonhole *Or:* a function from one finite set to a smaller finite set cannot be one-to-one **2.** if n pigeons fly into m pigeonholes and, for some positive integer k, $km < n$, then at least one pigeonhole contains $k + 1$ or more pigeons *Or:* for any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $km < n$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of Y **3.** f is onto

9.5 Counting Subsets of a Set: Combinations

"But 'glory' doesn't mean 'a nice knock-down argument,'" Alice objected. "When I use a word," Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean—neither more nor less." —Lewis Carroll, *Through the Looking Glass*, 1872

Consider the following question:

> Suppose 5 members of a group of 12 are to be chosen to work as a team on a special project. How many distinct 5-person teams can be selected?

This question is answered in Example 9.5.4. It is a special case of the following more general question:

> Given a set S with n elements, how many subsets of size r can be chosen from S?

The number of subsets of size r that can be chosen from S equals the number of subsets of size r that S has. Each individual subset of size r is called an *r-combination* of the set.

Note Although there is a convenient formula for computing values of $\binom{n}{r}$, it is helpful to think of $\binom{n}{r}$ simply as a way to count the number of subsets of size r that can be formed from a set of n elements.

Definition *r*-combination

Let n and r be nonnegative integers with $r \leq n$. An ***r*-combination** of a set of n elements is a subset of r of the n elements.

Notation $\binom{n}{r}$

The symbol $\binom{n}{r}$, read "n choose r," denotes the number of subsets of size r (or r-combinations) that can be formed from a set of n elements.

As noted in Section 5.1, calculators generally use symbols like $C(n, r)$, ${}_nC_r$, $C_{n,r}$, or ${}^nC_r$ instead of $\binom{n}{r}$.

Example 9.5.1 **3-Combinations**

Consider a set consisting of 4 people: Ann, Bob, Cyd, and Dan.

a. Given the set {Ann, Bob, Cyd, and Dan}, each subset of size 3 is a 3-combination of its elements. List all the 3-combinations of the set.

b. Use the result of part (a) to find $\binom{4}{3}$.

c. In how many ways can the people in the set form a committee of size 3?

Solution

a. Each 3-combination (subset of size 3) can be obtained by leaving out one of the elements of the set:

{Bob, Cyd, Dan} leave out Ann
{Ann, Cyd, Dan} leave out Bob
{Ann, Bob, Dan} leave out Cyd
{Ann, Bob, Cyd} leave out Dan.

b. There are 4 items in the list of 3-combinations in part (a). So, $\binom{4}{3} = 4$.

c. The number of ways for the people in the set to form a committee of size 3 is the number of distinct such committees, which is the same as the number of subsets of size 3 and equals the number of 3-combinations of elements in the set. Thus there are 4 ways the people in the set can form a committee of size 3. ■

There are two distinct methods that can be used to select r objects from a set of n elements. In an **ordered selection**, it is not only what elements are chosen but also the order in which they are chosen that matters. Two ordered selections are said to be the same if the elements chosen are the same and also if the elements are chosen in the same order. An ordered selection of r elements from a set of n elements is an r-permutation of the set.

In an **unordered selection**, on the other hand, it is only the identity of the chosen elements that matters. Two unordered selections are said to be the same if they consist of the same elements, regardless of the order in which the elements are chosen. An unordered selection of r elements from a set of n elements is the same as a subset of size r or an r-combination of the set.

Example 9.5.2 **Unordered Selections**

How many unordered selections of two elements can be made from the set {0, 1, 2, 3}?

Solution An unordered selection of two elements from {0, 1, 2, 3} is the same as a 2-combination, or subset of size 2, taken from the set. These can be listed systematically:

{0, 1}, {0, 2}, {0, 3}	subsets containing 0
{1, 2}, {1, 3}	subsets containing 1 but not already listed
{2, 3}	subsets containing 2 but not already listed.

Since this listing exhausts all possibilities, there are six subsets in all. Thus $\binom{4}{2} = 6$, which is the number of unordered selections of two elements from a set of four. ■

When the values of n and r are small, it is reasonable to calculate values of $\binom{n}{r}$ using the method of **complete enumeration** (listing all possibilities), which was illustrated in Examples 9.5.1 and 9.5.2. But when n and r are large, it is not feasible to compute these numbers by listing and counting all possibilities.

The general values of $\binom{n}{r}$ can be found by a somewhat indirect but simple method. An equation is derived that contains $\binom{n}{r}$ as a factor. Then this equation is solved to obtain a formula for $\binom{n}{r}$. The method is illustrated by Example 9.5.3.

Example 9.5.3 **Relation between Permutations and Combinations**

Write all 2-permutations of the set {0, 1, 2, 3}. Find an equation relating the number of 2-permutations, $P(4, 2)$, and the number of 2-combinations, $\binom{4}{2}$, and solve this equation for $\binom{4}{2}$.

Solution According to Theorem 9.2.3, the number of 2-permutations of the set {0, 1, 2, 3} is $P(4, 2)$, which equals

$$\frac{4!}{(4-2)!} = \frac{4 \cdot 3 \cdot \cancel{2!}}{\cancel{2!}} = 12.$$

Now the act of constructing a 2-permutation of {0, 1, 2, 3} can be thought of as a two-step process:

Step 1: Choose a subset of two elements from {0, 1, 2, 3}.

Step 2: Choose an ordering for the two-element subset.

This process can be illustrated by the possibility tree shown in Figure 9.5.1.

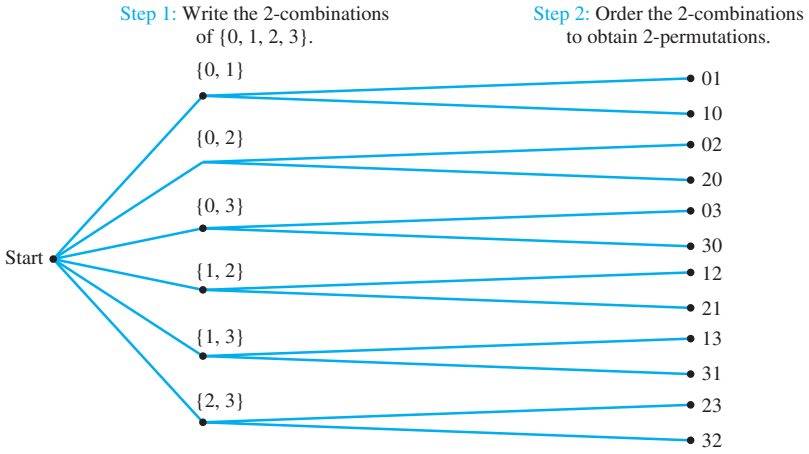


FIGURE 9.5.1 Relation between Permutations and Combinations

The number of ways to perform step 1 is $\binom{4}{2}$, the same as the number of subsets of size 2 that can be chosen from {0, 1, 2, 3}. The number of ways to perform step 2 is 2!, the number of ways to order the elements in a subset of size 2. Because the number of ways of performing the whole process is the number of 2-permutations of the set {0, 1, 2, 3}, which equals $P(4, 2)$, it follows from the product rule that

$$P(4, 2) = \binom{4}{2} \cdot 2!. \quad \text{This is an equation that relates } P(4, 2) \text{ and } \binom{4}{2}.$$

Solving the equation for $\binom{4}{2}$ gives

$$\binom{4}{2} = \frac{P(4, 2)}{2!}$$

Recall that $P(4, 2) = \frac{4!}{(4-2)!}$ So, substituting yields

$$\binom{4}{2} = \frac{\dfrac{4!}{(4-2)!}}{2!} = \frac{4!}{2!(4-2)!} = 6.$$ ■

The reasoning used in Example 9.5.3 applies in the general case as well. To form an r-permutation of a set of n elements, first choose a subset of r of the n elements (there are $\binom{n}{r}$ ways to perform this step), and then choose an ordering for the r elements (there are $r!$ ways to perform this step). Thus the number of r-permutations is

$$P(n, r) = \binom{n}{r} \cdot r!.$$

Now solve for $\binom{n}{r}$ to obtain the formula

$$\binom{n}{r} = \frac{P(n, r)}{r!}.$$

Since $P(n, r) = \frac{n!}{(n-r)!}$, substitution gives

$$\binom{n}{r} = \frac{\dfrac{n!}{(n-r)!}}{r!} = \frac{n!}{r!(n-r)!}.$$

The result of this discussion is summarized and extended in Theorem 9.5.1.

Theorem 9.5.1 Computational Formula for $\binom{n}{r}$

The number of subsets of size r (or r-combinations) that can be chosen from a set of n elements, $\binom{n}{r}$, is given by the formula

$$\binom{n}{r} = \frac{P(n, r)}{r!} \qquad \text{first version}$$

or, equivalently,

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} \qquad \text{second version}$$

where n and r are nonnegative integers with $r \leq n$.

Note that the analysis presented before the theorem proves the theorem in all cases where n and r are positive. If r is zero and n is any nonnegative integer, then $\binom{n}{0}$ is the number of subsets of size zero of a set with n elements. But you know from Section 6.2 that there is only one set that does not have any elements. Consequently, $\binom{n}{0} = 1$. Also

$$\frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1$$

since $0! = 1$ by definition. (Remember we said that definition would turn out to be convenient!) Hence the formula

$$\binom{n}{0} = \frac{n!}{0!(n-0)!}$$

holds for every integer $n \geq 0$, and so the theorem is true for all nonnegative integers n and r with $r \leq n$.

Example 9.5.4 **Calculating the Number of Teams**

Consider again the problem of choosing five members from a group of twelve to work as a team on a special project. How many distinct five-person teams can be chosen?

Solution The number of distinct five-person teams is the same as the number of subsets of size 5 (or 5-combinations) that can be chosen from the set of 12. This number is $\binom{12}{5}$. By Theorem 9.5.1,

$$\binom{12}{5} = \frac{12!}{5!(12-5)!} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7!}{(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1) \cdot 7!} = 11 \cdot 9 \cdot 8 = 792.$$

Thus there are 792 distinct five-person teams. ■

The formula for the number of r-combinations of a set can be applied in a wide variety of situations. Some of these are illustrated in the following examples.

Example 9.5.5 **Teams That Contain Both or Neither**

Suppose two members of the group of 12 insist on working as a pair—any team must contain either both or neither. How many five-person teams can be formed?

Solution Call the two members of the group that insist on working as a pair A and B. Then any team formed must contain both A and B or neither A nor B. The set of all possible teams can be partitioned into two subsets as shown in Figure 9.5.2 below.

A team that contains both A and B looks like

$$\underline{A} \quad \underline{B} \quad \underline{?} \quad \underline{?} \quad \underline{?}$$

where the three question marks are replaced by three people from the remaining ten in the group. Hence there are as many such teams as there are subsets of three people that can be chosen from the remaining ten, and by Theorem 9.5.1, this number is

$$\binom{10}{3} = \frac{10!}{3! \cdot 7!} = \frac{10 \cdot \overset{3}{\cancel{9}} \cdot \overset{4}{\cancel{8}} \cdot 7!}{\cancel{3} \cdot \cancel{2} \cdot 1 \cdot 7!} = 120.$$

A team that contains neither A nor B looks like

$$\underline{?} \quad \underline{?} \quad \underline{?} \quad \underline{?} \quad \underline{?}$$

where the five question marks are replaced by five people from the remaining ten. Thus there are as many such teams as there are subsets of five people that can be chosen from the remaining ten, and by Theorem 9.5.1, this number is

$$\binom{10}{5} = \frac{10!}{5! \cdot 5!} = \frac{\overset{2}{\cancel{10}} \cdot 9 \cdot \overset{2}{\cancel{8}} \cdot 7 \cdot 6 \cdot \cancel{5!}}{\cancel{5} \cdot 4 \cdot \cancel{3} \cdot \cancel{2} \cdot 1 \cdot \cancel{5!}} = 252.$$

Because the set of teams that contain both A and B is disjoint from the set of teams that contain neither A nor B, by the addition rule,

$$\begin{bmatrix}\text{the number of teams}\\ \text{containing both } A \text{ and } B\\ \text{or neither } A \text{ nor } B\end{bmatrix} = \begin{bmatrix}\text{the number of teams}\\ \text{containing}\\ \text{both } A \text{ and } B\end{bmatrix} + \begin{bmatrix}\text{the number of teams}\\ \text{containing}\\ \text{neither } A \text{ nor } B\end{bmatrix}$$
$$= 120 + 252 = 372.$$

This reasoning is summarized in Figure 9.5.2.

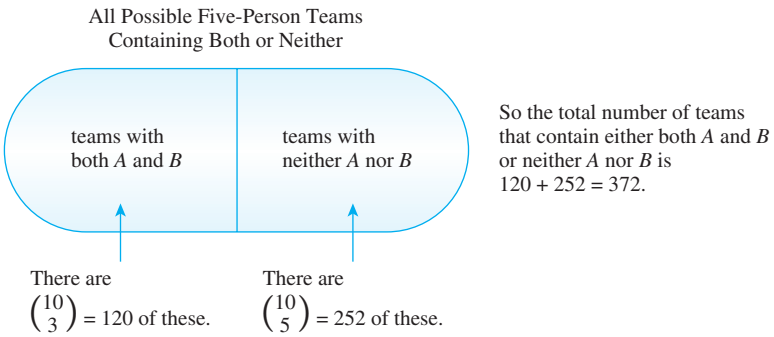


FIGURE 9.5.2 ■

Example 9.5.6 **Teams That Do Not Contain Both**

Suppose two members of the group don't get along and refuse to work together on a team. How many five-person teams can be formed?

Solution Call the two people who refuse to work together C and D. There are two different ways to answer the given question: One uses the addition rule and the other uses the difference rule.

To use the addition rule, partition the set of all teams that don't contain both C and D into three subsets as shown in Figure 9.5.3 below.

Because any team that contains C but not D contains exactly four other people from the remaining ten in the group, by Theorem 9.5.1 the number of such teams is

$$\binom{10}{4} = \frac{10!}{4!(10-4)!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6!}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 6!} = 210.$$

Similarly, there are $\binom{10}{4} = 210$ teams that contain D but not C. Finally, by the same reasoning as in Example 9.5.5, there are 252 teams that contain neither C nor D. Thus, by the addition rule,

$$\begin{bmatrix}\text{the number of teams that do}\\ \text{not contain both } C \text{ and } D\end{bmatrix} = 210 + 210 + 252 = 672.$$

This reasoning is summarized in Figure 9.5.3.

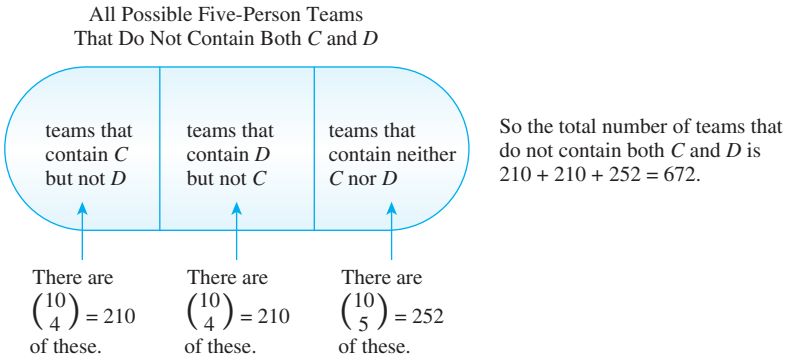


FIGURE 9.5.3

The alternative solution by the difference rule is based on the following observation: The set of all five-person teams that don't contain both C and D equals the set difference between the set of all five-person teams and the set of all five-person teams that contain both C and D. By Example 9.5.4, the total number of five-person teams is $\binom{12}{5} = 792$. Thus, by the difference rule,

$$\begin{bmatrix}\text{the number of teams that don't}\\ \text{contain both } C \text{ and } D\end{bmatrix} = \begin{bmatrix}\text{the total number of}\\ \text{teams of five}\end{bmatrix} - \begin{bmatrix}\text{the number of teams that}\\ \text{contain both } C \text{ and } D\end{bmatrix}$$
$$= \binom{12}{5} - \binom{10}{3} = 792 - 120 = 672.$$

This reasoning is summarized in Figure 9.5.4.

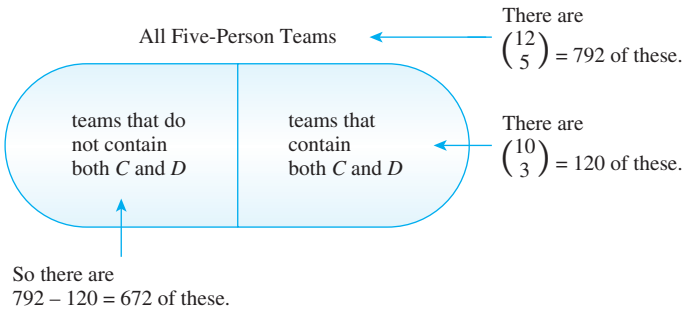


FIGURE 9.5.4

Before we begin the next example, a remark on the phrases *at least* and *at most* is in order:

> The phrase **at least *n*** means "*n* or more."
>
> The phrase **at most *n*** means "*n* or fewer."

For instance, if a set consists of three elements and you are to choose at least two, you will choose two or three; if you are to choose at most two, you will choose none, or one, or two.

Example 9.5.7 **Teams with Members of Two Types**

Suppose the group of twelve consists of five men and seven women.

a. How many five-person teams can be chosen that consist of three men and two women?

b. How many five-person teams contain at least one man?

c. How many five-person teams contain at most one man?

Solution

a. To answer this question, think of forming a team as a two-step process:

Step 1: Choose the men.

Step 2: Choose the women.

There are $\binom{5}{3}$ ways to choose the three men out of the five and $\binom{7}{2}$ ways to choose the two women out of the seven. Hence, by the product rule,

$$\begin{bmatrix}\text{the number of teams of five that}\\ \text{contain three men and two women}\end{bmatrix} = \binom{5}{3}\binom{7}{2} = \frac{5!}{3!2!}\cdot\frac{7!}{2!5!}$$

$$= \frac{5!\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3!}{3!\cdot 2\cdot 1\cdot 2\cdot 1\cdot 5!}$$

$$= 210.$$

b. This question can also be answered either by the addition rule or by the difference rule. The solution by the difference rule is shorter and is shown first.

Observe that the set of five-person teams containing at least one man equals the set difference between the set of all five-person teams and the set of five-person teams that do not contain any men. See Figure 9.5.5 on the next page.

Now a team with no men consists entirely of five women chosen from the seven women in the group, so there are $\binom{7}{5}$ such teams. Also, by Example 9.5.4, the total number of five-person teams is $\binom{12}{5} = 792$. Hence, by the difference rule,

$$\begin{bmatrix}\text{the number of teams}\\ \text{with at least}\\ \text{one man}\end{bmatrix} = \begin{bmatrix}\text{the total number}\\ \text{of teams}\\ \text{of five}\end{bmatrix} - \begin{bmatrix}\text{the number of teams}\\ \text{of five that do not}\\ \text{contain any men}\end{bmatrix}$$

$$= \binom{12}{5} - \binom{7}{5} = 792 - \frac{7!}{5!\cdot 2!}$$

$$= 792 - \frac{7\cdot \overset{3}{\cancel{6}}\cdot \cancel{5!}}{\cancel{5!}\cdot \cancel{2}\cdot 1} = 792 - 21 = 771.$$

This reasoning is summarized in Figure 9.5.5.

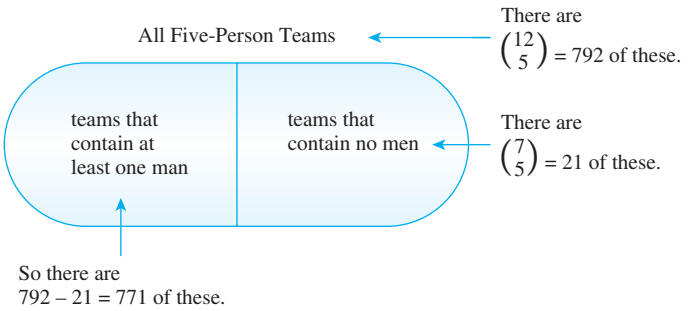


FIGURE 9.5.5

Alternatively, to use the addition rule, observe that the set of teams containing at least one man can be partitioned as shown in Figure 9.5.6. The number of teams in each subset of the partition is calculated using the method illustrated in part (a). There are

$\binom{5}{1}\binom{7}{4}$ teams with one man and four women

$\binom{5}{2}\binom{7}{3}$ teams with two men and three women

$\binom{5}{3}\binom{7}{2}$ teams with three men and two women

$\binom{5}{4}\binom{7}{1}$ teams with four men and one woman

$\binom{5}{5}\binom{7}{0}$ teams with five men and no women.

Hence, by the addition rule,

$$\begin{bmatrix}\text{the number of teams}\\ \text{with at least one man}\end{bmatrix}$$

$$= \binom{5}{1}\binom{7}{4} + \binom{5}{2}\binom{7}{3} + \binom{5}{3}\binom{7}{2} + \binom{5}{4}\binom{7}{1} + \binom{5}{5}\binom{7}{0}$$

$$= \frac{5!}{1!4!}\cdot\frac{7!}{4!3!} + \frac{5!}{2!3!}\cdot\frac{7!}{3!4!} + \frac{5!}{3!2!}\cdot\frac{7!}{2!5!} + \frac{5!}{4!1!}\cdot\frac{7!}{1!6!} + \frac{5!}{5!0!}\cdot\frac{7!}{0!7!}$$

$$= \frac{5\cdot 4!\cdot 7\cdot 6\cdot 5\cdot 4!}{1\cdot 4!\cdot 4!\cdot 3\cdot 2\cdot 1} + \frac{5\cdot \overset{2}{4}\cdot 3!\cdot 7\cdot 6\cdot 5\cdot 4!}{2\cdot 1\cdot 3!\cdot 3\cdot 2\cdot 1\cdot 4!} + \frac{5\cdot 4\cdot 3!\cdot 7\cdot 6\cdot 5!}{3!\cdot 2\cdot 1\cdot 2\cdot 1\cdot 5!} + \frac{5\cdot 4!\cdot 7\cdot 6!}{4!\cdot 6!} + \frac{5!\cdot 7!}{5!\cdot 7!}$$

$$= 5\cdot 7\cdot 5 + 5\cdot 2\cdot 7\cdot 5 + 5\cdot 7\cdot 6 + 5\cdot 7 + 1 = 175 + 350 + 210 + 35 + 1 = 771.$$

This reasoning is summarized in Figure 9.5.6.

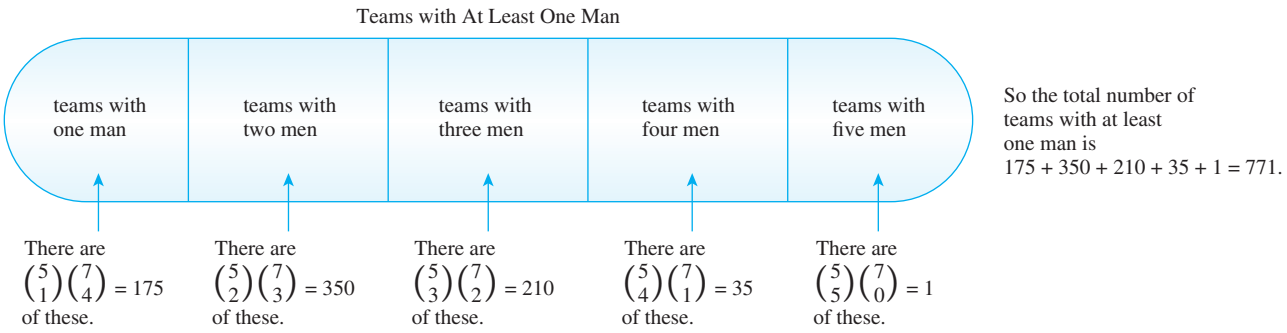


FIGURE 9.5.6

c. As shown in Figure 9.5.7, the set of teams containing at most one man can be partitioned into the set without any men and the set with exactly one man. Hence, by the addition rule,

$$\begin{bmatrix}\text{the number of teams}\\ \text{with at}\\ \text{most one man}\end{bmatrix} = \begin{bmatrix}\text{the number of}\\ \text{teams without}\\ \text{any men}\end{bmatrix} + \begin{bmatrix}\text{the number of}\\ \text{teams with}\\ \text{one man}\end{bmatrix}$$

$$= \binom{5}{0}\binom{7}{5} + \binom{5}{1}\binom{7}{4} = 21 + 175 = 196.$$

This reasoning is summarized in Figure 9.5.7.

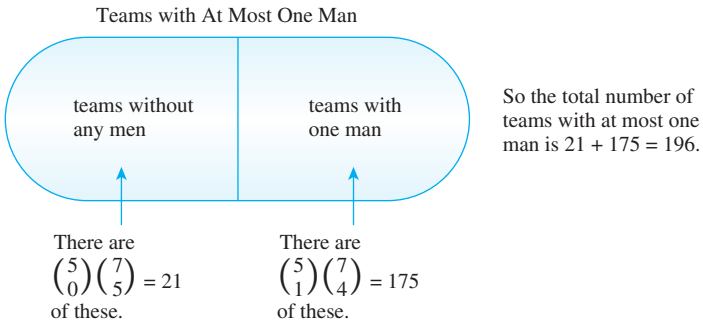


FIGURE 9.5.7

■

Example 9.5.8 **An Application to Graphs**

a. Use the multiplication rule to show that $K_{m,n}$, a complete bipartite graph on (m, n) vertices, has mn edges.

b. Use 2-combinations to show that K_n, a complete graph on n vertices, has $\frac{n(n-1)}{2}$ edges.

Solution

a. A complete bipartite graph on (m, n) vertices, K_{mn}, is a simple graph whose vertices can be divided into two distinct, nonoverlapping sets—say, V with m vertices and W with n vertices—in such a way that there is exactly one edge from each vertex of V to each vertex of W, there is no edge from any one vertex of V to any other vertex of V, and there is no edge from any one vertex of W to any other vertex of W. Label the m vertices of V as $v_1, v_2, \ldots, v_m$. Think of constructing the edges between the vertices of V and the vertices of W as an m-step process: for each integer k from 1 through m, draw exactly one edge from v_k to each of the n edges of W. Because each step can be performed in n ways and there are m steps, by the multiplication rule there are mn ways to construct all the edges. Thus $K_{m,n}$ has mn edges.

b. A complete graph on n vertices, K_n, is a simple graph with n vertices and exactly one edge between each pair of vertices. If $n = 1$, then K_n has one vertex and 0 edges, and since $\frac{n(n-1)}{2} = \frac{1(1-1)}{2} = 0$, then K_n has $\frac{n(n-1)}{2}$ edges. If $n \geq 2$, then, since any two distinct vertices of K_n are connected by exactly one edge, there are as many edges in K_n as there are subsets of size two in the set of n vertices. By Theorem 9.5.1, there are $\binom{n}{2}$ such sets, and

$$\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$$

Hence K_n has $\frac{n(n-1)}{2}$ edges. ■

Example 9.5.9 **Poker Hand Problems**

The game of poker is played with an ordinary deck of 52 cards (see Example 9.1.1). Various five-card holdings are given special names, and certain holdings beat certain other holdings. The named holdings are listed from highest to lowest below.

Royal flush: 10, J, Q, K, A of the same suit

Straight flush: five adjacent denominations of the same suit but not a royal flush—aces can be high or low, so A, 2, 3, 4, 5 of the same suit is a straight flush

Four of a kind: four cards of one denomination—the fifth card can be any other in the deck

Full house: three cards of one denomination, two cards of another denomination

Flush: five cards of the same suit but not a straight or a royal flush

Straight: five cards of adjacent denominations but not all of the same suit—aces can be high or low

Three of a kind: three cards of the same denomination and two other cards of different denominations

Two pairs: two cards of one denomination, two cards of a second denomination, and a fifth card of a third denomination

One pair: two cards of one denomination and three other cards all of different denominations

No pairs: all cards of different denominations but not a straight, or straight flush, or flush, or royal flush

a. How many five-card poker hands contain two pairs?

b. If a five-card hand is dealt at random from an ordinary deck of cards, what is the probability that the hand contains two pairs?

Solution

a. Consider forming a hand with two pairs as a four-step process:

Step 1: Choose the two denominations for the pairs.

Step 2: Choose two cards from the smaller denomination.

Step 3: Choose two cards from the larger denomination.

Step 4: Choose one card from those remaining.

The number of ways to perform step 1 is $\binom{13}{2}$ because there are 13 denominations in all. The number of ways to perform each of steps 2 and 3 is $\binom{4}{2}$ because there are four cards of each denomination, one in each suit. The number of ways to perform step 4 is $\binom{44}{1}$ because the fifth card is chosen from the eleven denominations not included in the pair and there are four cards of each denomination. Thus

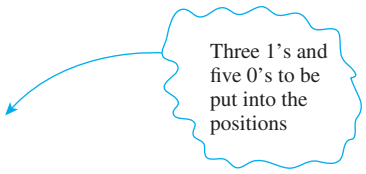
$$\begin{aligned}\left[\begin{matrix}\text{the total number of}\\ \text{hands with two pairs}\end{matrix}\right] &= \binom{13}{2}\binom{4}{2}\binom{4}{2}\binom{44}{1}\\ &= \frac{13!}{2!(13-2)!}\cdot\frac{4!}{2!(4-2)!}\cdot\frac{4!}{2!(4-2)!}\cdot\frac{44!}{1!(44-1)!}\\ &= \frac{13\cdot 12\cdot 11!}{(2\cdot 1)\cdot 11!}\cdot\frac{4\cdot 3\cdot 2!}{(2\cdot 1)\cdot 2!}\cdot\frac{4\cdot 3\cdot 2!}{(2\cdot 1)\cdot 2!}\cdot\frac{44\cdot 43!}{1\cdot 43!}\\ &= 78\cdot 6\cdot 6\cdot 44 = 123{,}552.\end{aligned}$$

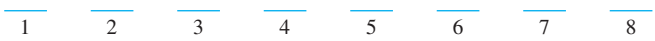
b. The total number of five-card hands from an ordinary deck of cards is $\binom{52}{5}$, which equals 2,598,960. Thus if all hands are equally likely, the probability of obtaining a hand with two pairs is $\frac{123{,}552}{2{,}598{,}960} \cong 4.75\%$.

Example 9.5.10 **Number of Bit Strings with Fixed Number of 1's**

How many eight-bit strings have exactly three 1's?

Solution To solve this problem, imagine eight empty positions into which the 0's and 1's of the bit string will be placed. In step 1, choose positions for the three 1's, and in step 2, put the 0's into place.





Once a subset of three positions has been chosen from the eight to contain 1's, then the remaining five positions must all contain 0's (since the string is to have exactly three 1's). It follows that the number of ways to construct an eight-bit string with exactly three 1's is the same as the number of subsets of three positions that can be chosen from the eight into

which to place the 1's. By Theorem 9.5.1, this equals

$$\binom{8}{3} = \frac{8!}{3! \cdot 5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5!}{3 \cdot 2 \cdot 5!} = 56.$$

■

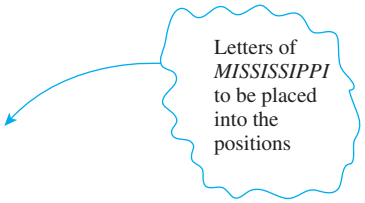
Example 9.5.11 **Permutations of a Set with Repeated Elements**

Consider various ways of ordering the letters in the word *MISSISSIPPI*:

IIMSSPISSIP, *ISSSPMIIPIS*, *PIMISSSSIIP*, and so on.

How many distinguishable orderings are there?

Solution This example generalizes Example 9.5.10. Imagine placing the 11 letters of *MISSISSIPPI* one after another into 11 positions.



1 2 3 4 5 6 7 8 9 10 11

Because copies of the same letter cannot be distinguished from one another, once the positions for a certain letter are known, then all copies of the letter can go into the positions in any order. It follows that constructing an ordering for the letters can be thought of as a four-step process:

Step 1: Choose a subset of four positions for the *S*'s.

Step 2: Choose a subset of four positions for the *I*'s.

Step 3: Choose a subset of two positions for the *P*'s.

Step 4: Choose a subset of one position for the *M*.

Since there are 11 positions in all, there are $\binom{11}{4}$ subsets of four positions for the *S*'s. Once the four *S*'s are in place, there are seven positions that remain empty, so there are $\binom{7}{4}$ subsets of four positions for the *I*'s. After the *I*'s are in place, there are three positions left empty, so there are $\binom{3}{2}$ subsets of two positions for the *P*'s. That leaves just one position for the *M*. But $1 = \binom{1}{1}$. Hence by the multiplication rule,

$$\left[\begin{array}{l}\text{number of ways to}\\ \text{position all the letters}\end{array}\right] = \binom{11}{4}\binom{7}{4}\binom{3}{2}\binom{1}{1}$$

$$= \frac{11!}{4! \cdot 7!} \cdot \frac{7!}{4! \cdot 3!} \cdot \frac{3!}{2! \cdot 1!} \cdot \frac{1!}{1! \cdot 0!}$$

$$= \frac{11!}{4! \cdot 4! \cdot 2! \cdot 1!} = 34{,}650.$$

■

In exercise 18 at the end of the section, you are asked to show that changing the order in which the letters are placed into the positions does not change the answer to this example.

The same reasoning used in this example can be used to derive the following general theorem.

Theorem 9.5.2 Permutations with Sets of Indistinguishable Objects

Suppose a collection consists of n objects of which

n_1 are of type 1 and are indistinguishable from each other
n_2 are of type 2 and are indistinguishable from each other
$\vdots$
n_k are of type k and are indistinguishable from each other,

and suppose that $n_1 + n_2 + \cdots + n_k = n$. Then the number of distinguishable permutations of the n objects is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\cdots n_k!}.$$

Some Advice about Counting

Students learning counting techniques often ask, "How do I know what to multiply and what to add? When do I use the multiplication rule and when do I use the addition rule?" Unfortunately, these questions have no easy answers. You need to imagine, as vividly as possible, the objects you are to count. In fact, it is helpful to start making a list of the items you need to count to get a sense for how to obtain them in a systematic way. You should then construct a model that would allow you to continue counting the objects one by one if you had enough time. If you can imagine the elements to be counted as being obtained through a multistep process (in which each step is performed in a fixed number of ways regardless of how preceding steps were performed), then you can use the multiplication rule. The total number of elements will be the product of the number of ways to perform each step. If, however, you can imagine the set of elements to be counted as being broken up into disjoint subsets, then you can use the addition rule. The total number of elements in the set will be the sum of the number of elements in each subset.

One of the most common mistakes students make is to count certain possibilities more than once.

Example 9.5.12 **Double Counting**

Caution! Be careful to avoid counting items twice when using the multiplication rule.

Consider again the problem of Example 9.5.7(b). A group consists of five men and seven women. How many teams of five contain at least one man?

Incorrect Solution

Imagine constructing the team as a two-step process:

Step 1: Choose a subset of one man from the five men.

Step 2: Choose a subset of four others from the remaining eleven people.

Hence, by the multiplication rule, there are $\binom{5}{1}\cdot\binom{11}{4} = 1{,}650$ five-person teams that contain at least one man.

Analysis of the Incorrect Solution The problem with the solution above is that some teams are counted more than once. Suppose the men are Anwar, Ben, Carlos, Dwayne, and

Ed and the women are Fumiko, Gail, Hui-Fan, Inez, Jill, Kim, and Laura. According to the method described previously, one possible outcome of the two-step process is as follows:

Outcome of step 1: Anwar

Outcome of step 2: Ben, Gail, Inez, and Jill.

In this case the team would be {Anwar, Ben, Gail, Inez, Jill}. But another possible outcome is

Outcome of step 1: Ben

Outcome of step 2: Anwar, Gail, Inez, and Jill,

which also gives the team {Anwar, Ben, Gail, Inez, Jill}. Thus this one team is given by two different branches of the possibility tree, and so it is counted twice. ■

The best way to avoid mistakes such as the one just described is to visualize the possibility tree that corresponds to any use of the multiplication rule and the set partition that corresponds to a use of the addition rule. Check how your division into steps works by applying it to some actual data—as was done in the analysis above—and try to pick data that are as typical or generic as possible.

It often helps to ask yourself (1) "Am I counting everything?" and (2) "Am I counting anything twice?" When using the multiplication rule, these questions become (1) "Does every outcome appear as some branch of the tree?" and (2) "Does any outcome appear on more than one branch of the tree?" When using the addition rule, the questions become (1) "Does every outcome appear in some subset of the diagram?" and (2) "Do any two subsets in the diagram share common elements?"

TEST YOURSELF

1. The number of subsets of size r that can be formed from a set with n elements is denoted _____, which is read as "_____."
2. The number of r-combinations of a set of n elements is _____.
3. Two unordered selections are said to be the same if the elements chosen are the same, regardless of _____.
4. A formula relating $\binom{n}{r}$ and $p(n, r)$ is _____.
5. The phrase "at least n" means _____, and the phrase "at most n" means _____.

EXERCISE SET 9.5

1. **a.** List all 2-combinations for the set $\{x_1, x_2, x_3\}$. Deduce the value of $\binom{3}{2}$.
   b. List all unordered selections of four elements from the set $\{a, b, c, d, e\}$. Deduce the value of $\binom{5}{4}$.
2. **a.** List all 3-combinations for the set $\{x_1, x_2, x_3, x_4, x_5\}$. Deduce the value of $\binom{5}{3}$.
   b. List all unordered selections of two elements from the set $\{x_1, x_2, x_3, x_4, x_5, x_6\}$. Deduce the value of $\binom{6}{2}$.
3. Write an equation relating $P(7, 2)$ and $\binom{7}{2}$.
4. Write an equation relating $P(8, 3)$ and $\binom{8}{3}$.
5. Use Theorem 9.5.1 to compute each of the following.
   a. $\binom{6}{0}$ **b.** $\binom{6}{1}$ **c.** $\binom{6}{2}$
   d. $\binom{6}{3}$ **e.** $\binom{6}{4}$ **f.** $\binom{6}{5}$ **g.** $\binom{6}{6}$
6. A student council consists of 15 students.
   a. In how many ways can a committee of six be selected from the membership of the council?
   b. Two council members have the same major and are not permitted to serve together on a committee. How many ways can a committee

of six be selected from the membership of the council?

c. Two council members always insist on serving on committees together. If they can't serve together, they won't serve at all. How many ways can a committee of six be selected from the council membership?

d. Suppose the council contains eight men and seven women.
(i) How many committees of six contain three men and three women?
(ii) How many committees of six contain at least one woman?

e. Suppose the council consists of three freshmen, four sophomores, three juniors, and five seniors. How many committees of eight contain two representatives from each class?

7. A computer programming team has 13 members.

a. How many ways can a group of seven be chosen to work on a project?

b. Suppose seven team members are women and six are men.
(i) How many groups of seven can be chosen that contain four women and three men?
(ii) How many groups of seven can be chosen that contain at least one man?
(iii) How many groups of seven can be chosen that contain at most three women?

c. Suppose two team members refuse to work together on projects. How many groups of seven can be chosen to work on a project?

d. Suppose two team members insist on either working together or not at all on projects. How many groups of seven can be chosen to work on a project?

H **8.** An instructor gives an exam with fourteen questions. Students are allowed to choose any ten to answer.

a. How many different choices of ten questions are there?

b. Suppose six questions require proof and eight do not.
(i) How many groups of ten questions contain four that require proof and six that do not?
(ii) How many groups of ten questions contain at least one that requires proof?
(iii) How many groups of ten questions contain at most three that require proof?

c. Suppose the exam instructions specify that at most one of questions 1 and 2 may be included among the ten. How many different choices of ten questions are there?

d. Suppose the exam instructions specify that either both questions 1 and 2 are to be included among the ten or neither is to be included. How many different choices of ten questions are there?

9. A club is considering changing its bylaws. In an initial straw vote on the issue, 24 of the 40 members of the club favored the change and 16 did not. A committee of six is to be chosen from the 40 club members to devote further study to the issue.

a. What is the total number of committees of six that can be formed from the club membership?

b. How many of the total number of committees will contain at least three club members who, in the preliminary survey, favored the change in the bylaws?

10. Two new drugs are to be tested using a group of 60 laboratory mice, each tagged with a number for identification purposes. Drug *A* is to be given to 22 mice, drug *B* is to be given to another 22 mice, and the remaining 16 mice are to be used as controls. How many ways can the assignment of treatments to mice be made? (A single assignment involves specifying the treatment for each mouse—whether drug *A*, drug *B*, or no drug.)

* **11.** Refer to Example 9.5.9. For each poker holding below, (1) find the number of five-card poker hands with that holding; (2) find the probability that a randomly chosen set of five cards has that holding.

a. royal flush **b.** straight flush
c. four of a kind **d.** full house **e.** flush
f. straight (including a straight flush and a royal flush)
g. three of a kind **h.** one pair
i. neither a repeated denomination nor five of the same suit nor five adjacent denominations

12. How many pairs of two distinct integers chosen from the set $\{1, 2, 3, \ldots, 101\}$ have a sum that is even?

13. A coin is tossed ten times. In each case the outcome *H* (for heads) or *T* (for tails) is recorded. (One possible outcome of the ten tosses is denoted *T H H T T T H T T H*.)

a. What is the total number of possible outcomes of the coin-tossing experiment?

b. In how many of the possible outcomes are exactly five heads obtained?

c. In how many of the possible outcomes are at least eight heads obtained?
d. In how many of the possible outcomes is at least one head obtained?
e. In how many of the possible outcomes is at most one head obtained?

14. a. How many 16-bit strings contain exactly seven 1's?
b. How many 16-bit strings contain at least thirteen 1's?
c. How many 16-bit strings contain at least one 1?
d. How many 16-bit strings contain at most one 1?

15. a. How many even integers are in the set

$$\{1, 2, 3, \ldots, 100\}?$$

b. How many odd integers are in the set

$$\{1, 2, 3, \ldots, 100\}?$$

c. How many ways can two integers be selected from the set $\{1, 2, 3, \ldots, 100\}$ so that their sum is even?
d. How many ways can two integers be selected from the set $\{1, 2, 3, \ldots, 100\}$ so that their sum is odd?

16. Suppose that three microchips in a production run of forty are defective. A sample of five is to be selected to be checked for defects.
a. How many different samples can be chosen?
b. How many samples will contain at least one defective chip?
c. What is the probability that a randomly chosen sample of five contains at least one defective chip?

17. Ten points labeled $A, B, C, D, E, F, G, H, I, J$ are arranged in a plane in such a way that no three lie on the same straight line.
a. How many straight lines are determined by the ten points?
b. How many of these straight lines do not pass through point A?
c. How many triangles have three of the ten points as vertices?
d. How many of these triangles do not have point A as a vertex?

18. Suppose that you placed the letters in Example 9.5.11 into positions in the following order: first the *M*, then the *I*'s, then the *S*'s, and then the *P*'s. Show that you would obtain the same answer for the number of distinguishable orderings.

19. a. How many distinguishable ways can the letters of the word *HULLABALOO* be arranged in order?
b. How many distinguishable orderings of the letters of *HULLABALOO* begin with *U* and end with *L*?
c. How many distinguishable orderings of the letters of *HULLABALOO* contain the two letters *HU* next to each other in order?

20. a. How many distinguishable ways can the letters of the word *MILLIMICRON* be arranged in order?
b. How many distinguishable orderings of the letters of *MILLIMICRON* begin with *M* and end with *N*?
c. How many distinguishable orderings of the letters of *MILLIMICRON* contain the letters *CR* next to each other in order and also the letters *ON* next to each other in order?

21. In Morse code, symbols are represented by variable-length sequences of dots and dashes. (For example, $A = \cdot-$, $1 = \cdot - - - -$, $? = \cdot\cdot - -\cdot\cdot$.) How many different symbols can be represented by sequences of seven or fewer dots and dashes?

22. Each symbol in the Braille code is represented by a rectangular arrangement of six dots, each of which may be raised or flat against a smooth background. For instance, when the word Braille is spelled out, it looks like this:

Given that at least one of the six dots must be raised, how many symbols can be represented in the Braille code?

23. On an 8×8 chessboard, a rook is allowed to move any number of squares either horizontally or vertically. How many different paths can a rook follow from the bottom-left square of the board to the top-right square of the board if all moves are to the right or upward?

24. The number 42 has the prime factorization $2 \cdot 3 \cdot 7$. Thus 42 can be written in four ways as a product of two positive integer factors (without regard to

the order of the factors): $1 \cdot 42$, $2 \cdot 21$, $3 \cdot 14$, and $6 \cdot 7$. Answer a–d below without regard to the order of the factors.

a. List the distinct ways the number 210 can be written as a product of two positive integer factors.

b. If $n = p_1 p_2 p_3 p_4$, where the p_i are distinct prime numbers, how many ways can n be written as a product of two positive integer factors?

c. If $n = p_1 p_2 p_3 p_4 p_5$, where the p_i are distinct prime numbers, how many ways can n be written as a product of two positive integer factors?

d. If $n = p_1 p_2 \ldots p_k$, where the p_i are distinct prime numbers, how many ways can n be written as a product of two positive integer factors?

25. a. How many one-to-one functions are there from a set with three elements to a set with four elements?

b. How many one-to-one functions are there from a set with three elements to a set with two elements?

c. How many one-to-one functions are there from a set with three elements to a set with three elements?

d. How many one-to-one functions are there from a set with three elements to a set with five elements?

***H* e.** How many one-to-one functions are there from a set with m elements to a set with n elements, where $m \leq n$?

26. a. How many onto functions are there from a set with three elements to a set with two elements?

b. How many onto functions are there from a set with three elements to a set with five elements?

***H* c.** How many onto functions are there from a set with three elements to a set with three elements?

d. How many onto functions are there from a set with four elements to a set with two elements?

e. How many onto functions are there from a set with four elements to a set with three elements?

***H** f.** Let $c_{m,n}$ be the number of onto functions from a set of m elements to a set of n elements, where $m \geq n \geq 1$. Find a formula relating $c_{m,n}$ to $c_{m-1,n}$ and $c_{m-1,n-1}$.

27. Let A be a set with eight elements.

a. How many relations are there on A?

b. How many relations on A are reflexive?

c. How many relations on A are symmetric?

d. How many relations on A are both reflexive and symmetric?

***H*28.** A student council consists of three freshmen, four sophomores, four juniors, and five seniors. How many committees of eight members of the council contain at least one member from each class?

*** 29.** An alternative way to derive Theorem 9.5.1 uses the following *division rule*: Let n and k be integers so that k divides n. If a set consisting of n elements is divided into subsets that each contain k elements, then the number of such subsets is n/k. Explain how Theorem 9.5.1 can be derived using the division rule.

30. Find the error in the following reasoning: "Consider forming a poker hand with two pairs as a five-step process.

Step 1: Choose the denomination of one of the pairs.
Step 2: Choose the two cards of that denomination.
Step 3: Choose the denomination of the other of the pairs.
Step 4: Choose the two cards of that second denomination.
Step 5: Choose the fifth card from the remaining denominations.

There are $\binom{13}{1}$ ways to perform step 1, $\binom{4}{2}$ ways to perform step 2, $\binom{12}{1}$ ways to perform step 3, $\binom{4}{2}$ ways to perform step 4, and $\binom{44}{1}$ ways to perform step 5. Therefore, the total number of five-card poker hands with two pairs is $13 \cdot 6 \cdot 12 \cdot 6 \cdot 44 = 247{,}104$."

ANSWERS FOR TEST YOURSELF

1. $\binom{n}{r}$; n choose r **2.** $\binom{n}{r}$ (*Or:* n choose r) **3.** the order in which they are chosen **4.** $\binom{n}{r} = \dfrac{P(n, r)}{r!}$ **5.** n or more; n or fewer

9.6 *r*-Combinations with Repetition Allowed

The value of mathematics in any science lies more in disciplined analysis and abstract thinking than in particular theories and techniques. —Alan Tucker, 1982

In Section 9.5 we showed that there are $\binom{n}{r}$ r-combinations, or subsets of size r, of a set of n elements. In other words, there are $\binom{n}{r}$ ways to choose r distinct elements without regard to order from a set of n elements. For instance, there are $\binom{4}{3} = 4$ ways to choose three elements out of a set of four: {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}.

In this section we ask: How many ways are there to choose r elements without regard to order from a set of n elements *if repetition is allowed*? A good way to imagine this is to visualize the n elements as categories of objects from which multiple selections may be made. For instance, if the categories are labeled 1, 2, 3, and 4 and three elements are chosen, it is possible to choose two elements of type 3 and one of type 1, or all three of type 2, or one each of types 1, 2, and 4, and so forth. We denote such choices by [3, 3, 1], [2, 2, 2], and [1, 2, 4], respectively. Note that because order does not matter, [3, 3, 1] = [3, 1, 3] = [1, 3, 3], for example.

Definition and Notation

An *r-combination with repetition allowed*, or *multiset of size r*, chosen from a set X of n elements is an unordered selection of elements taken from X with repetition allowed. If $X = \{x_1, x_2, \ldots, x_n\}$, we write an r-combination with repetition allowed, or multiset of size r, as $[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other.

Example 9.6.1 ***r*-Combinations with Repetition Allowed**

Write a complete list to find the number of 3-combinations with repetition allowed, or multisets of size 3, that can be selected from {1, 2, 3, 4}. Observe that because the order in which the elements are chosen does not matter, the elements of each selection may be written in increasing order, and writing the elements in increasing order will ensure that no combinations are overlooked.

Solution

[1, 1, 1]; [1, 1, 2]; [1, 1, 3]; [1, 1, 4]	all combinations that start with 1, 1
[1, 2, 2]; [1, 2, 3]; [1, 2, 4];	all additional combinations that start with 1, 2
[1, 3, 3]; [1, 3, 4]; [1, 4, 4];	all additional combinations that start with 1, 3 or 1, 4
[2, 2, 2]; [2, 2, 3]; [2, 2, 4];	all additional combinations that start with 2, 2
[2, 3, 3]; [2, 3, 4]; [2, 4, 4];	all additional combinations that start with 2, 3 or 2, 4
[3, 3, 3]; [3, 3, 4]; [3, 4, 4];	all additional combinations that start with 3, 3 or 3, 4
[4, 4, 4]	the only additional combination that starts with 4, 4.

Thus there are twenty 3-combinations with repetition allowed. ■

How could the number twenty have been predicted other than by making a complete list? Consider the numbers 1, 2, 3, and 4 as categories and imagine choosing a total of three numbers from the categories with multiple selections from any category allowed. The results of several such selections are represented by the table on the next page.

Category 1	Category 2	Category 3	Category 4	Result of the Selection
|	× |	|	× ×	one from category 2 two from category 4
× |	|	× |	×	one each from categories 1, 3, and 4
× × × |	|	|		three from category 1

As you can see, each selection of three numbers from the four categories can be represented by a string of vertical bars and crosses. Three vertical bars are used to separate the four categories, and three crosses are used to indicate how many items from each category are chosen. Each distinct string of three vertical bars and three crosses represents a distinct selection. For instance, the string

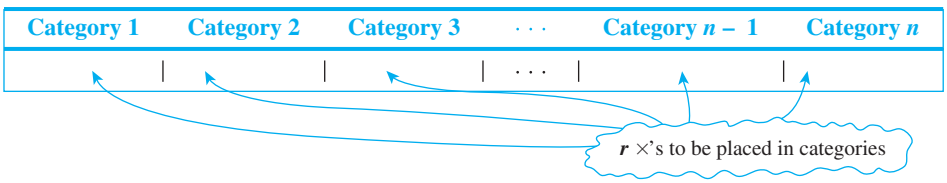
$$\times\ \times\ |\ |\ \times\ |$$

represents the selection: two from category 1, none from category 2, one from category 3, and none from category 4. Thus the number of distinct selections of three elements that can be formed from the set {1, 2, 3, 4} with repetition allowed equals the number of distinct strings of six symbols consisting of three |'s and three ×'s. And this equals the number of ways to select three positions out of six because once three positions have been chosen for the ×'s, the |'s are placed in the remaining three positions. Thus the answer is

$$\binom{6}{3} = \frac{6!}{3!(6-3)!} = \frac{6\cdot 5\cdot 4\cdot 3!}{3\cdot 2\cdot 1\cdot 3!} = 20,$$

as was obtained earlier by a careful listing.

The analysis of this example extends to the general case. To count the number of r-combinations with repetition allowed, or multisets of size r, that can be selected from a set of n elements, think of the elements of the set as categories. Then each r-combination with repetition allowed can be represented as a string of $n-1$ vertical bars (to separate the n categories) and r crosses (to represent the r elements to be chosen). The number of ×'s in each category represents the number of times the element represented by that category is repeated.



The number of strings of $n-1$ vertical bars and r crosses is the number of ways to choose r positions, into which to place the r crosses, out of a total of $r+(n-1)$ positions, leaving the remaining positions for the vertical bars. And by Theorem 9.5.1, this number is $\binom{r+n-1}{r}$.

This discussion proves the following theorem.

Theorem 9.6.1

The number of r-combinations with repetition allowed (or multisets of size r) that can be selected from a set of n elements is

$$\binom{r+n-1}{r}.$$

This equals the number of ways r objects can be selected from n categories of objects with repetition allowed.

Example 9.6.2 **Selecting 15 Cans of Soft Drinks of Five Different Types**

A person giving a party wants to set out 15 assorted cans of soft drinks for his guests. He shops at a store that sells five different types of soft drinks.

a. How many different selections of cans of 15 soft drinks can he make?

b. If root beer is one of the types of soft drink, how many different selections include at least six cans of root beer?

c. If the store has only five cans of root beer but at least 15 cans of each other type of soft drink, how many different selections are there?

Solution

a. Think of the five different types of soft drinks as the n categories and the 15 cans of soft drinks to be chosen as the r objects (so $n = 5$ and $r = 15$). Each selection of cans of soft drinks is represented by a string of $5 - 1 = 4$ vertical bars (to separate the categories of soft drinks) and 15 crosses (to represent the cans selected). For instance, the string

$$\times\ \times\ \times\ |\ \times\ \times\ \times\ \times\ \times\ \times\ \times\ |\ |\ \times\ \times\ \times\ |\ \times\ \times$$

represents a selection of three cans of soft drinks of type 1, seven of type 2, none of type 3, three of type 4, and two of type 5. The total number of selections of 15 cans of soft drinks of the five types is the number of strings of 19 symbols, $5 - 1 = 4$ of them $|$ and 15 of them $\times$:

$$\binom{15+5-1}{15} = \frac{19!}{15!\cdot(19-15)!} = \binom{19}{15} = \frac{19\cdot \overset{6}{\cancel{18}}\cdot 17\cdot \overset{2}{\cancel{16}}\cdot \cancel{15}!}{\cancel{15}!\cdot \cancel{4}\cdot \cancel{3}\cdot \cancel{2}\cdot 1} = 3{,}876.$$

b. If at least six cans of root beer are to be included in the selection, you can imagine choosing six such cans first and then choosing nine additional cans. The choice of the nine additional cans can be represented as a string of 9 $\times$'s and 4 $|$'s. For example, if root beer is type 1, then the string $\times\ \times\ \times\ |\ |\ \times\ \times\ |\ \times\ \times\ \times\ \times\ |$ represents a selection of three cans of root beer (in addition to the six chosen initially), none of type 2, two of type 3, four of type 4, and none of type 5. Thus the total number of selections of 15 cans of soft drinks of the five types, including at least six cans of root beer, is the number of strings of 13 symbols, 4 ($=5-1$) of them $|$ and 9 of them $\times$:

$$\binom{9+4}{9} = \frac{13!}{9!\cdot(13-9)!} = \binom{13}{9} = \frac{13\cdot \cancel{12}\cdot 11\cdot \overset{5}{\cancel{10}}\cdot \cancel{9}!}{\cancel{9}!\cdot \cancel{4}\cdot \cancel{3}\cdot \cancel{2}\cdot 1} = 715.$$

c. If the store has only five cans of root beer, then the number of different selections of 15 cans of soft drinks of the five types is the same as the number of different selections that contain five or fewer cans of root beer. Let T be the set of all possible selections assuming that there are at least 15 cans of each type, let $R_{\leq 5}$ be the set of selections from T that contain five or fewer cans of root beer, and let $R_{\geq 6}$ be the set of selections from T that contain six or more cans of root beer. Then

$$T = R_{\leq 5} \cup R_{\geq 6} \quad \text{and} \quad R_{\leq 5} \cap R_{\geq 6} = \varnothing.$$

By part (a) $N(T) = 3{,}876$ and by part (b) $N(R_{\geq 6}) = 715$. Thus, by the difference rule,

$$N(R_{\leq 5}) = N(T) - N(R_{\geq 6}) = 3{,}876 - 715 = 3{,}161.$$

So, when there are only five or fewer cans of root beer, the number of different selections of soft drinks is 3,161. ■

Example 9.6.3 **Counting Triples (i, j, k) with $1 \leq i \leq j \leq k \leq n$**

If n is a positive integer, how many triples of integers from 1 through n can be formed in which the elements of the triple are written in increasing order but are not necessarily distinct? In other words, how many triples of integers (i, j, k) are there with $1 \leq i \leq j \leq k \leq n$?

Solution Any triple of integers (i, j, k) with $1 \leq i \leq j \leq k \leq n$ can be represented as a string of $n - 1$ vertical bars and three crosses, with the positions of the crosses indicating which three integers from 1 to n are included in the triple. The table below illustrates this for $n = 5$.

Category					Result of the Selection
1	2	3	4	5	
|	|	× × |	|	×	(3, 3, 5)
× |	× |	|	|	|	(1, 2, 4)

Thus the number of such triples is the same as the number of strings of $(n-1)$ |'s and 3 ×'s, which is

$$\binom{3+(n-1)}{3} = \binom{n+2}{3} = \frac{(n+2)!}{3!(n+2-3)!}$$

$$= \frac{(n+2)(n+1)n(n-1)!}{3!(n-1)!} = \frac{n(n+1)(n+2)}{6}.$$ ■

Note that in Examples 9.6.2 and 9.6.3 the reasoning behind Theorem 9.6.1 was used rather than the statement of the theorem itself. Alternatively, in either example we could invoke Theorem 9.6.1 directly by recognizing that the items to be counted either are r-combinations with repetition allowed or are the same in number as such combinations. For instance, in Example 9.6.3 we might observe that there are exactly as many triples of integers (i, j, k) with $1 \leq i \leq j \leq k \leq n$ as there are 3-combinations of integers from 1 through n with repetition allowed because the elements of any such 3-combination can be written in increasing order in only one way.

Example 9.6.4 **Counting Iterations of a Loop**

How many times will the innermost loop be iterated when the algorithm segment below is implemented and run? (Assume n is a positive integer.)

```
for k := 1 to n
    for j := 1 to k
        for i := 1 to j
            [Statements in the body of the inner loop,
            none containing branching statements that lead
            outside the loop]
        next i
    next j
next k
```

Solution Construct a trace table for the values of k, j, and i for which the statements in the body of the innermost loop are executed.

k	1	2	→	→	3	→	→	→	→	→	⋯	n	→	→	→	→	→	→
j	1	1	2	→	1	2	→	3	→	→	⋯	1	2	→	⋯	n	→	→
i	1	1	1	2	1	1	2	1	2	3	⋯	1	1	2	⋯	1	⋯	n

Because i goes from 1 to j, it is always the case that $i \le j$. Similarly, because j goes from 1 to k, it is always the case that $j \le k$. To focus on the details of the table construction, consider what happens when $k = 3$. In this case, j takes each value 1, 2, and 3. When $j = 1$, i can only take the value 1 (because $i \le j$). When $j = 2$, i takes each value 1 and 2 (again because $i \le j$). When $j = 3$, i takes each value 1, 2, and 3 (yet again because $i \le j$).

Observe that there is one iteration of the innermost loop for each column of the table, and there is one column of the table for each triple of integers (i, j, k) with $1 \le i \le j \le k \le n$. Now Example 9.6.3 showed that the number of such triples is $[n(n+1)(n+2)]/6$. Thus there are $[n(n+1)(n+2)]/6$ iterations of the innermost loop. ■

The solution in Example 9.6.4 is elegant and generalizable. (See exercises 8 and 9.) An alternative solution using summations is outlined in exercise 21.

Example 9.6.5 **The Number of Integral Solutions of an Equation**

How many solutions are there to the equation $x_1 + x_2 + x_3 + x_4 = 10$ if x_1, x_2, x_3, and x_4 are nonnegative integers?

Solution Think of the number 10 as divided into ten individual units and the variables x_1, x_2, x_3, and x_4 as four categories into which these units are placed. The number of units in each category x_i indicates the value of x_i in a solution of the equation. Each solution can, then, be represented by a string of three vertical bars (to separate the four categories) and ten crosses (to represent the ten individual units). For example, in the following table, the two crosses under x_1, five crosses under x_2, and three crosses under x_4 represent the solution $x_1 = 2$, $x_2 = 5$, $x_3 = 0$, and $x_4 = 3$.

Categories				Solution to the Equation $x_1 + x_2 + x_3 + x_4 = 10$
x_1	x_2	x_3	x_4	
× × |	× × × × × |	|	× × ×	$x_1 = 2$, $x_2 = 5$, $x_3 = 0$, and $x_4 = 3$
× × × × |	× × × × × × |	|		$x_1 = 4$, $x_2 = 6$, $x_3 = 0$, and $x_4 = 0$

Therefore, there are as many solutions to the equation as there are strings of ten crosses and three vertical bars, namely,

$$\binom{10+3}{10} = \binom{13}{10} = \frac{13!}{10!(13-10)!} = \frac{13\cdot 12\cdot 11\cdot \cancel{10!}}{\cancel{10!}\cdot 3\cdot 2\cdot 1} = 286. \quad \blacksquare$$

Example 9.6.6 illustrates a variation on Example 9.6.5.

Example 9.6.6 **Additional Constraints on the Number of Solutions**

How many integer solutions are there to the equation $x_1 + x_2 + x_3 + x_4 = 10$ if each $x_i \geq 1$?

Solution In this case imagine starting by putting one cross in each of the four categories. Then distribute the remaining six crosses among the categories. Such a distribution can be represented by a string of three vertical bars and six crosses. For example, the string

$$\times\times\times|\ \ |\times\times|\times$$

indicates that there are three more crosses in category x_1 in addition to the one cross already there (so $x_1 = 4$), no more crosses in category x_2 in addition to the one already there (so $x_2 = 1$), two more crosses in category x_3 in addition to the one already there (so $x_3 = 3$), and one more cross in category x_4 in addition to the one already there (so $x_4 = 2$). It follows that the number of solutions to the equation that satisfy the given condition is the same as the number of strings of three vertical bars and six crosses, namely,

$$\binom{6+3}{6} = \binom{9}{6} = \frac{9!}{6!(9-6)!} = \frac{9\cdot 8\cdot 7\cdot \cancel{6!}}{\cancel{6!}\cdot 3\cdot 2\cdot 1} = 84.$$

An alternative solution to this example is based on the observation that since each $x_i \geq 1$, we may introduce new variables $y_i = x_i - 1$ for each $i = 1, 2, 3, 4$. Then each $y_i \geq 0$, and $y_1 + y_2 + y_3 + y_4 = 6$. Thus the number of solutions of $y_1 + y_2 + y_3 + y_4 = 6$ in nonnegative integers is the same as the number of solutions of $x_1 + x_2 + x_3 + x_4 = 10$ in positive integers. $\blacksquare$

Remark: Deciding Which Formula to Use

In Sections 9.2, 9.3, 9.5, and 9.6 we discussed four different ways of choosing k elements from n. The order in which the choices are made may or may not matter, and repetition may or may not be allowed. The following table summarizes which formula to use in which situation.

	Order Matters	**Order Does Not Matter**
Repetition Is Allowed	n^k	$\binom{k+n-1}{k}$
Repetition Is Not Allowed	$P(n, k)$	$\binom{n}{k}$

TEST YOURSELF

1. Given a set $X = \{x_1, x_2, \ldots, x_n\}$, an r-combination with repetition allowed, or a multiset of size r, chosen from X is _____, which is denoted _____.

2. If $X = \{x_1, x_2, \ldots, x_n\}$, the number of r-combinations with repetition allowed (or multisets of size r) chosen from X is _____.

3. When choosing k elements from a set of n elements, order may or may not matter and repetition may or may not be allowed.
   - The number of ways to choose the k elements when repetition is allowed and order matters is _____.
   - The number of ways to choose the k elements when repetition is not allowed and order matters is _____.
   - The number of ways to choose the k elements when repetition is not allowed and order does not matter is _____.
   - The number of ways to choose the k elements when repetition is allowed and order does not matter is _____.

EXERCISE SET 9.6

1. **a.** According to Theorem 9.6.1, how many 5-combinations with repetition allowed can be chosen from a set of three elements?
   b. List all of the 5-combinations that can be chosen with repetition allowed from the set $\{1, 2, 3\}$.

2. **a.** According to Theorem 9.6.1, how many multisets of size four can be chosen from a set of three elements?
   b. List all of the multisets of size four that can be chosen from the set $\{x, y, z\}$.

3. A bakery produces six different kinds of pastry, one of which is éclairs. Assume there are at least 20 pastries of each kind.
   a. How many different selections of twenty pastries are there?
   b. How many different selections of twenty pastries are there if at least three must be éclairs?
   c. How many different selections of twenty pastries contain at most two éclairs?

4. A camera shop stocks eight different types of batteries, one of which is type A76. Assume there are at least 30 batteries of each type.
   a. How many ways can a total inventory of 30 batteries be distributed among the eight different types?
   b. How many ways can a total inventory of 30 batteries be distributed among the eight different types if the inventory must include at least four A76 batteries?
   c. How many ways can a total inventory of 30 batteries be distributed among the eight different types if the inventory includes at most three A76 batteries?

5. If n is a positive integer, how many 4-tuples of integers from 1 through n can be formed in which the elements of the 4-tuple are written in increasing order but are not necessarily distinct? In other words, how many 4-tuples of integers (i, j, k, m) are there with $1 \le i \le j \le k \le m \le n$?

6. If n is a positive integer, how many 5-tuples of integers from 1 through n can be formed in which the elements of the 5-tuple are written in decreasing order but are not necessarily distinct? In other words, how many 5-tuples of integers (h, i, j, k, m) are there with $n \ge h \ge i \ge j \ge k \ge m \ge 1$?

7. Another way to count the number of nonnegative integral solutions to an equation of the form $x_1 + x_2 + \cdots + x_n = m$ is to reduce the problem to one of finding the number of n-tuples $(y_1, y_2, \ldots, y_n)$ with $0 \le y_1 \le y_2 \le \cdots \le y_n \le m$. The reduction results from letting $y_i = x_1 + x_2 + \cdots + x_i$ for each $i = 1, 2, \ldots, n$. Use this approach to derive a general formula for the number of nonnegative integral solutions to $x_1 + x_2 + \cdots + x_n = m$.

In 8 and 9, how many times will the innermost loop be iterated when the algorithm segment is implemented and run? Assume *n*, *m*, *k*, and *j* are positive integers.

8.
```
for m := 1 to n
    for k := 1 to m
        for j := 1 to k
            for i := 1 to j
                [Statements in the body of the inner
                loop, none containing branching
                statements that lead outside the
                loop]
            next i
        next j
    next k
next m
```

9.
```
for k := 1 to n
    for j := k to n
        for i := j to n
            [Statements in the body of the inner loop,
            none containing branching statements
            that lead outside the loop]
        next i
    next j
next k
```

In 10–14, find how many solutions there are to the given equation that satisfy the given condition.

10. $x_1 + x_2 + x_3 = 20$, each x_i is a nonnegative integer.

11. $x_1 + x_2 + x_3 = 20$, each x_i is a positive integer.

12. $y_1 + y_2 + y_3 + y_4 = 30$, each y_i is a nonnegative integer.

13. $y_1 + y_2 + y_3 + y_4 = 30$, each y_i is an integer that is at least 2.

14. $a + b + c + d + e = 500$, each of a, b, c, d, and e is an integer that is at least 10.

***15.** For how many integers from 1 through 99,999 is the sum of their digits equal to 10?

16. Consider the situation in Example 9.6.2.
- **a.** Suppose the store has only six cans of lemonade but at least 15 cans of each of the other four types of soft drink. In how many different ways can fifteen cans of soft drink be selected?
- **b.** Suppose that the store has only five cans of root beer and only six cans of lemonade but at least 15 cans of each of the other three types of soft drink. In how many different ways can fifteen cans of soft drink be selected?

***H* 17.**
- **a.** A store sells 8 colors of balloons with at least 30 of each color. How many different combinations of 30 balloons can be chosen?
- **b.** If the store has only 12 red balloons but at least 30 of each other color of balloon, how many combinations of balloons can be chosen?
- **c.** If the store has only 8 blue balloons but at least 30 of each other color of balloon, how many combinations of balloons can be chosen?
- **d.** If the store has only 12 red balloons and only 8 blue balloons but at least 30 of each other color of balloon, how many combinations of balloons can be chosen?

18. A large pile of coins consists of pennies, nickels, dimes, and quarters.
- **a.** How many different collections of 30 coins can be chosen if there are at least 30 of each kind of coin?
- **b.** If the pile contains only 15 quarters but at least 30 of each other kind of coin, how many collections of 30 coins can be chosen?
- **c.** If the pile contains only 20 dimes but at least 30 of each other kind of coin, how many collections of 30 coins can be chosen?
- **d.** If the pile contains only 15 quarters and only 20 dimes but at least 30 of each other kind of coin, how many collections of 30 coins can be chosen?

***H* 19.** Suppose the bakery in exercise 3 has only ten éclairs but has at least twenty of each of the other kinds of pastry.
- **a.** How many different selections of twenty pastries are there?
- **b.** Suppose in addition to having only ten éclairs, the bakery has only eight napoleon slices. How many different selections of twenty pastries are there?

20. Suppose the camera shop in exercise 4 can obtain at most ten A76 batteries but can get at least 30 of each of the other types.
- **a.** How many ways can a total inventory of 30 batteries be distributed among the eight different types?
- **b.** Suppose that in addition to being able to obtain only ten A76 batteries, the store can get only six of type D303. How many ways can a total inventory of 30 batteries be distributed among the eight different types?

21. Observe that the number of columns in the trace table for Example 9.6.4 can be expressed as the sum

$$1 + (1 + 2) + (1 + 2 + 3) + \cdots + (1 + 2 + \cdots + n).$$

Explain why this is so, and show how this sum simplifies to the same expression given in the solution of Example 9.6.4. (*Hint:* A formula from exercise 13 in Section 5.2 will be helpful.)

ANSWERS FOR TEST YOURSELF

1. an unordered selection of elements taken from X with repetition allowed; $[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other **2.** $\binom{r+n-1}{r}$ **3.** n^k; $n(n-1)(n-2)\cdots(n-k+1)$ (*Or:* $P(n, k)$); $\binom{n}{k}$; $\binom{k+n-1}{k}$

9.7 Pascal's Formula and the Binomial Theorem

I'm very well acquainted, too, with matters mathematical, I understand equations both the simple and quadratical. About binomial theorem I am teaming with a lot of news.
—William S. Gilbert, *The Pirates of Penzance*, 1880

In this section we derive several formulas for values of $\binom{n}{r}$. The most important is Pascal's formula, which is the basis for Pascal's triangle and is a crucial component of one of the proofs of the binomial theorem. We offer two distinct proofs for both Pascal's formula and the binomial theorem. One of them is called "algebraic" because it relies to a great extent on algebraic manipulation, and the other is called "combinatorial," because it is based on the kind of counting arguments we have been discussing in this chapter.

Example 9.7.1 **Values of $\binom{n}{n}, \binom{n}{n-1}, \binom{n}{n-2}$**

Think of Theorem 9.5.1 as a general template: Regardless of what nonnegative integers are placed in the boxes, if the integer in the lower box is no greater than the integer in the top box, then

$$\binom{\square}{\diamond} = \frac{\square!}{\diamond!(\square - \diamond)!}.$$

Use Theorem 9.5.1 to show that for every integer $n \geq 0$,

$$\binom{n}{n} = 1 \tag{9.7.1}$$

$$\binom{n}{n-1} = n, \quad \text{if } n \geq 1 \tag{9.7.2}$$

$$\binom{n}{n-1} = \frac{n(n-1)}{2}, \quad \text{if } n \geq 2. \tag{9.7.3}$$

Solution

$$\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{1}{0!} = 1 \quad \text{since } 0! = 1 \text{ by definition}$$

$$\binom{n}{n-1} = \frac{n!}{(n-1)!(n-(n-1))!}$$

$$= \frac{n \cdot (n-1)!}{(n-1)!(n-n+1)!} = \frac{n}{1} = n$$

$$\binom{n}{n-2} = \frac{n!}{(n-2)!(n-(n-2))!}$$

$$= \frac{n \cdot (n-1) \cdot (n-2)!}{(n-2)!2!} = \frac{n(n-1)}{2}$$

■

Note that the result derived algebraically above, that $\binom{n}{n}$ equals 1, agrees with the fact that a set with n elements has just one subset of size n, namely, itself. Similarly, exercise 1 at the end of the section asks you to show algebraically that $\binom{n}{0} = 1$, which agrees with the fact

that a set with n elements has one subset, the empty set, of size 0. In exercise 2 you are also asked to show algebraically that $\binom{n}{1} = n$. This result agrees with the fact that there are n subsets of size 1 that can be chosen from a set with n elements, namely the subsets consisting of each element taken alone.

Example 9.7.2 $\binom{n}{r} = \binom{n}{n-r}$

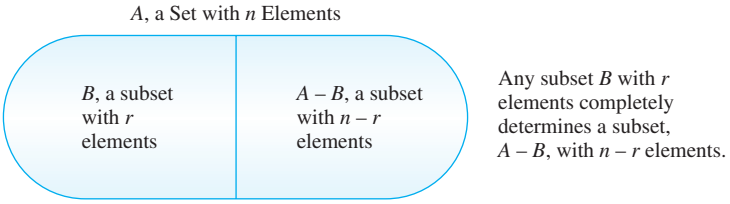
In exercise 5 at the end of the section you are asked to verify algebraically that

$$\binom{n}{r} = \binom{n}{n-r}$$

for all nonnegative integers n and r with $r \leq n$.

An alternative way to deduce this formula is to interpret it as saying that a set A with n elements has exactly as many subsets of size r as it has subsets of size $n - r$. Derive the formula using this reasoning.

Solution Observe that any subset of size r can be specified either by saying which r elements lie in the subset or by saying which $n - r$ elements lie outside the subset.



Suppose A has k subsets of size r: $B_1, B_2, \ldots, B_k$. Then each B_i can be paired up with exactly one set of size $n - r$, namely, its complement $A - B_i$, as shown below.

Subsets of Size r		Subsets of Size $n - r$
B_1	$\longleftrightarrow$	$A - B_1$
B_2	$\longleftrightarrow$	$A - B_2$
$\vdots$		$\vdots$
B_k	$\longleftrightarrow$	$A - B_k$

All subsets of size r are listed in the left-hand column, and all subsets of size $n - r$ are listed in the right-hand column. The number of subsets of size r equals the number of subsets of size $n - r$, and so $\binom{n}{r} = \binom{n}{n-r}$. ■

The type of reasoning used in this example is called *combinatorial*, because it is obtained by counting things that are combined in different ways. A number of theorems have both combinatorial proofs and proofs that are purely algebraic.

Hulton Deutsch/Getty Images

Blaise Pascal (1623–1662)

Pascal's Formula

Pascal's formula, named after the seventeenth-century French mathematician and philosopher Blaise Pascal, is one of the most famous and useful in combinatorics (which is the formal term for the study of counting and listing problems). It relates the value of $\binom{n+1}{r}$ to the values of $\binom{n}{r-1}$ and $\binom{n}{r}$. Specifically, it says that

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

whenever n and r are positive integers with $r \le n$. This formula makes it easy to compute higher combinations in terms of lower ones: If all the values of $\binom{n}{r}$ are known, then the values of $\binom{n+1}{r}$ can be computed for every integer r such that $0 < r \le n$.

Pascal's triangle, shown in Table 9.7.1, is a geometric version of Pascal's formula. Sometimes it is simply called the arithmetic triangle because it was used centuries before Pascal by Chinese and Persian mathematicians. But Pascal discovered it independently, and ever since 1654, when he published a treatise that explored many of its features, it has generally been known as Pascal's triangle.

TABLE 9.7.1 Pascal's Triangle for Values of $\binom{n}{r}$

n \ r	0	1	2	3	4	5	…	$r-1$	r	…
0	1							·	·	…
1	1							·	·	…
2	1	2	1					·	·	…
3	1	3	3	1				·	·	…
4	1	4	6	4	1			·	·	…
5	1	5	10	10	5	1		·	·	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮	⋮	⋮
n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	…	$\binom{n}{r-1}$	$\binom{n}{r}$	…
$n+1$	$\binom{n+1}{0}$	$\binom{n+1}{1}$	$\binom{n+1}{2}$	$\binom{n+1}{3}$	$\binom{n+1}{4}$	$\binom{n+1}{5}$	…		$\binom{n+1}{r}$	…
·		·	·	·	·	·		·	·	…
·		·	·	·	·	·		·	·	…
·		·	·	·	·	·		·	·	…

Each entry in the triangle is a value of $\binom{n}{r}$. Pascal's formula translates into the fact that the entry in row $n+1$, column r equals the sum of the entry in row n, column $r-1$ plus the entry in row n, column r. That is, the entry in a given interior position equals the sum of the two entries directly above and to the above left. The left-most and right-most entries in each row are 1 because $\binom{n}{n} = 1$ by Example 9.7.1 and $\binom{n}{0} = 1$ by exercise 1 at the end of this section.

Example 9.7.3 **Calculating $\binom{n}{r}$ Using Pascal's Triangle**

Use Pascal's triangle to compute the values of

$$\binom{6}{2} \quad \text{and} \quad \binom{6}{3}.$$

Solution By construction, the value in row n, column r of Pascal's triangle is the value of $\binom{n}{r}$, for every pair of positive integers n and r with $r \le n$. By Pascal's formula, $\binom{n+1}{r}$ can

be computed by adding together $\binom{n}{r-1}$ and $\binom{n}{r}$, which are located directly above and above left of $\binom{n+1}{r}$. Thus,

$$\binom{6}{2} = \binom{5}{1} + \binom{5}{2} = 5 + 10 = 15 \quad \text{and}$$

$$\binom{6}{3} = \binom{5}{2} + \binom{5}{3} = 10 + 10 = 20.$$ ■

Pascal's formula can be derived by two entirely different arguments. One is algebraic; it uses the formula for the number of r-combinations obtained in Theorem 9.5.1. The other is combinatorial; it uses the definition of the number of r-combinations as the number of subsets of size r taken from a set with a certain number of elements. We give both proofs since both approaches have applications in many other situations.

Theorem 9.7.1 Pascal's Formula

Let n and r be positive integers with $r \le n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Proof (algebraic version): Let n and r be positive integers with $r \le n$. We will show that the right-hand side of Pascal's formula equals its left-hand side. By Theorem 9.5.1,

$$\binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)!(n-(r-1))!} + \frac{n!}{r!(n-r)!}$$

$$= \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!}$$

To add these fractions, a common denominator is needed, so multiply the numerator and denominator of the left-hand fraction by r and multiply the numerator and denominator of the right-hand fraction by $(n-r+1)$. Then

$$\binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)!(n-r+1)!} \cdot \frac{r}{r} + \frac{n!}{r!(n-r)!} \cdot \frac{(n-r+1)}{(n-r+1)}$$

$$= \frac{n! \cdot r}{(n-r+1)! \cdot r(r-1)!} + \frac{n \cdot n! - n! \cdot r + n!}{(n-r+1)(n-r)! \cdot r!}$$

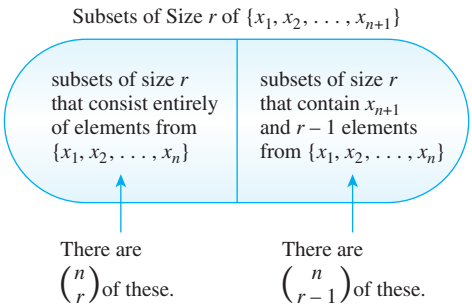
$$= \frac{\cancel{n! \cdot r} + n! \cdot n - \cancel{n! \cdot r} + n!}{(n-r+1)!r!} = \frac{n!(n+1)}{(n+1-r)!r!}$$

$$= \frac{(n+1)!}{((n+1)-r)!r!} = \binom{n+1}{r}.$$ This is what was to be shown.

Proof (combinatorial version): Let n and r be positive integers with $r \le n$. Suppose S is a set with $n+1$ elements. The number of subsets of S of size r can be calculated by thinking of S as consisting of two pieces: one with n elements $\{x_1, x_2, \ldots, x_n\}$ and the other with one element $\{x_{n+1}\}$.

Any subset of S with r elements either contains x_{n+1} or it does not. If it contains x_{n+1}, then it contains $r-1$ elements from the set $\{x_1, x_2, \ldots, x_n\}$. If it does not contain x_{n+1}, then it contains r elements from the set $\{x_1, x_2, \ldots, x_n\}$.

(continued on page 646)



By the addition rule,

$$\begin{bmatrix}\text{the number of subsets}\\ \text{of } \{x_1, x_2, \ldots, x_n, x_{n+1}\}\\ \text{of size } r\end{bmatrix} = \begin{bmatrix}\text{the number of subsets}\\ \text{of } \{x_1, x_2, \ldots, x_n\}\\ \text{of size } r-1\end{bmatrix} + \begin{bmatrix}\text{the number of subsets}\\ \text{of } \{x_1, x_2, \ldots, x_n\}\\ \text{of size } r\end{bmatrix}$$

By Theorem 9.5.1, the set $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$ has $\binom{n+1}{r}$ subsets of size r, the set $\{x_1, x_2, \ldots, x_n\}$ has $\binom{n}{r-1}$ subsets of size $r-1$, and the set $\{x_1, x_2, \ldots, x_n\}$ has $\binom{n}{r}$ subsets of size r. Thus

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r},$$

as was to be shown.

Example 9.7.4 **Deriving New Formulas from Pascal's Formula**

Use Pascal's formula to derive a formula for $\binom{n+2}{r}$ in terms of values of $\binom{n}{r}$, $\binom{n}{r-1}$, and $\binom{n}{r-2}$. Assume n and r are nonnegative integers and $2 \le r \le n$.

Solution By Pascal's formula,

$$\binom{n+2}{r} = \binom{n+1}{r-1} + \binom{n+1}{r}.$$

Now apply Pascal's formula to $\binom{n+1}{r-1}$ and $\binom{n+1}{r}$ and substitute into the above to obtain

$$\binom{n+2}{r} = \left[\binom{n}{r-2} + \binom{n}{r-1}\right] + \left[\binom{n}{r-1} + \binom{n}{r}\right].$$

Combining the two middle terms gives

$$\binom{n+2}{r} = \binom{n}{r-2} + 2\binom{n}{r-1} + \binom{n}{r}$$

for all nonnegative integers n and r such that $2 \le r \le n$. ■

The Binomial Theorem

In algebra a sum of two terms, such as $a + b$, is called a **binomial**. The *binomial theorem* gives an expression for the powers of a binomial $(a + b)^n$, for each nonnegative integer n and all real numbers a and b.

Consider what happens when you calculate the first few powers of $a + b$. According to the distributive law of algebra, you take the sum of the products of all combinations of individual terms:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = aa + ab + ba + bb,\\ (a+b)^3 &= (a+b)(a+b)(a+b)\\ &= aaa + aab + aba + abb + baa + bab + bba + bbb,\\ (a+b)^4 &= \underbrace{(a+b)(a+b)(a+b)(a+b)}_{\substack{\text{1st}\\ \text{factor}}\ \ \substack{\text{2nd}\\ \text{factor}}\ \ \substack{\text{3rd}\\ \text{factor}}\ \ \substack{\text{4th}\\ \text{factor}}}\\ &= aaaa + aaab + aaba + aabb + abaa + abab + abba + abbb\\ &\qquad + baaa + baab + baba + babb + bbaa + bbab + bbba + bbbb.\end{aligned}$$

Now focus on the expansion of $(a + b)^4$. (It is concrete, and yet it has all the features of the general case.) A typical term of this expansion is obtained by multiplying one of the two terms from the first factor times one of the two terms from the second factor times one of the two terms from the third factor times one of the two terms from the fourth factor. For example, the term $abab$ is obtained by multiplying the a's and b's marked with arrows below.

$$\overset{\downarrow}{(a}+\overset{\ }{b)}\overset{\ }{(a}+\overset{\downarrow}{b)}\overset{\downarrow}{(a}+\overset{\ }{b)}\overset{\ }{(a}+\overset{\downarrow}{b)}$$

Since there are two possible values—a or b—for each term selected from one of the four factors, there are $2^4 = 16$ terms in the expansion of $(a + b)^4$.

Now some terms in the expansion are "like terms" and can be combined. Consider all possible orderings of three a's and one b, for example. By the techniques of Section 9.5, there are $\binom{4}{1} = 4$ of them. And each of the four occurs as a term in the expansion of $(a + b)^4$:

$$aaab \quad aaba \quad abaa \quad baaa.$$

By the commutative and associative laws of algebra, each such term equals a^3b, so all four are "like terms." When the like terms are combined, therefore, the coefficient of a^3b equals $\binom{4}{1}$.

Similarly, the expansion of $(a + b)^4$ contains the $\binom{4}{2} = 6$ different orderings of two a's and two b's,

$$aabb \quad abab \quad abba \quad baab \quad baba \quad bbaa,$$

all of which equal a^2b^2, so the coefficient of a^2b^2 equals $\binom{4}{2}$. By a similar analysis, the coefficient of ab^3 equals $\binom{4}{3}$. Also, since there is only one way to order four a's, the coefficient of a^4 is 1 (which equals $\binom{4}{0}$), and since there is only one way to order four b's, the coefficient of b^4 is 1 (which equals $\binom{4}{4}$). Thus, when all of the like terms are combined,

$$\begin{aligned}(a+b)^4 &= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4\\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.\end{aligned}$$

The binomial theorem generalizes this formula to an arbitrary nonnegative integer n.

Theorem 9.7.2 Binomial Theorem

Given any real numbers a and b and any nonnegative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$
$$= a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n.$$

Note that the second expression equals the first because $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$, for every nonnegative integer n, since $b^0 = 1$ and $a^{n-n} = 1$.

It is instructive to see two proofs of the binomial theorem: an algebraic proof and a combinatorial proof. Both require a precise definition of integer power.

Definition

For any real number a and any nonnegative integer n, the **nonnegative integer powers of a** are defined as follows:

$$a^n = \begin{cases} 1 & \text{if } n = 0 \\ a \cdot a^{n-1} & \text{if } n > 0. \end{cases}$$

In some mathematical contexts, 0^0 is left undefined. Defining it to be 1, as indicated in Section 5.1, makes it possible to write general formulas such as $\sum_{i=0}^{n} x^i = \frac{1}{1-x}$ without having to exclude values of the variables that result in the expression 0^0.

The algebraic version of the binomial theorem uses mathematical induction and calls upon Pascal's formula at a crucial point.

Proof of the Binomial Theorem (algebraic version):

Suppose a and b are real numbers. We use mathematical induction and let the property $P(n)$ be the equation

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \qquad \leftarrow P(n)$$

Show that P(0) is true: When $n = 0$, the binomial theorem states that:

$$(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^{0-k} b^k. \qquad \leftarrow P(0)$$

Now the left-hand side is $(a+b)^0 = 1$ *[by definition of power]*, and the right-hand side is

$$\sum_{k=0}^{0} \binom{0}{k} a^{0-k} b^k = \binom{0}{0} a^{0-0} b^0$$
$$= \frac{0!}{0! \cdot (0-0)!} \cdot 1 \cdot 1 = \frac{1}{1 \cdot 1} = 1$$

also *[since* $0! = 1$, $a^0 = 1$, *and* $b^0 = 1$*]*. Hence $P(0)$ is true.

Show that for each integer $m \geq 0$, if $P(m)$ is true then $P(m+1)$ is true: Let m be any integer with $m \geq 0$, and suppose $P(m)$ is true. That is, suppose

$$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k. \qquad P(m) \text{ inductive hypothesis.}$$

We need to show that $P(m+1)$ is true:

$$(a+b)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} a^{(m+1)-k} b^k. \qquad P(m+1)$$

Now, by definition of the $(m+1)$st power,

$$(a+b)^{m+1} = (a+b)\cdot(a+b)^m,$$

so by substitution from the inductive hypothesis,

$$\begin{aligned}(a+b)^{m+1} &= (a+b)\cdot \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\ &= a\cdot \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k + b\cdot \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\ &= \sum_{k=0}^{m} \binom{m}{k} a^{m+1-k} b^k + \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^{k+1}\end{aligned}$$

by the generalized distributive law and the facts that $a\cdot a^{m-k} = a^{1+m-k} = a^{m+1-k}$ and $b\cdot b^k = b^{1+k} = b^{k+1}$.

We transform the second summation on the right-hand side by making the change of variable $j = k+1$. When $k = 0$, then $j = 1$. When $k = m$, then $j = m+1$. And since $k = j-1$, the general term is

$$\binom{m}{k} a^{m-k} b^{k+1} = \binom{m}{j-1} a^{m-(j-1)} b^j = \binom{m}{j-1} a^{m+1-j} b^j.$$

Hence the second summation on the right-hand side above is

$$\sum_{j=1}^{m+1} \binom{m}{j-1} a^{m+1-j} b^j.$$

But the j in this summation is a dummy variable; it can be replaced by the letter k, as long as the replacement is made everywhere the j occurs:

$$\sum_{j=1}^{m+1} \binom{m}{j-1} a^{m+1-j} b^j = \sum_{k=1}^{m+1} \binom{m}{k-1} a^{m+1-k} b^k.$$

Substituting back, we get

$$(a+b)^{m+1} = \sum_{k=0}^{m} \binom{m}{k} a^{m+1-k} b^k + \sum_{k=1}^{m+1} \binom{m}{k-1} a^{m+1-k} b^k.$$

[The reason for the above maneuvers was to make the powers of a and b agree so that we can add the summations together term by term, except for the first and the last terms, which we must write separately.]

(continued on page 650)

Thus

$$(a+b)^{m+1} = \binom{m}{0}a^{m+1-0}b^0 + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right]a^{m+1-k}b^k + \binom{m}{(m+1)-1}a^{m+1-(m+1)}b^{m+1}$$

$$= a^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right]a^{m+1-k}b^k + b^{m+1}$$

since $a^0 = b^0 = 1$ and $\binom{m}{0} = \binom{m}{m} = 1$.

But

$$\left[\binom{m}{k} + \binom{m}{k-1}\right] = \binom{m+1}{k}$$

by Pascal's formula.

Hence

$$(a+b)^{m+1} = a^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k}a^{(m+1)-k}b^k + b^{m+1}$$

$$= \sum_{k=0}^{m+1}\binom{m+1}{k}a^{(m+1)-k}b^k$$

because $\binom{m+1}{0} = \binom{m+1}{m+1} = 1$

This is what was to be shown.

It is instructive to write out the product $(a+b)\cdot(a+b)^m$ without using the summation notation but using the inductive hypothesis about $(a+b)^m$:

$$(a+b)^{m+1} = (a+b)\cdot\left[a^m + \binom{m}{1}a^{m-1}b + \cdots + \binom{m}{k-1}a^{m-(k-1)}b^{k-1} + \binom{m}{k}a^{m-k}b^k + \cdots + \binom{m}{m-1}ab^{m-1} + b^m\right].$$

You will see that the first and last coefficients are clearly 1 and that the term containing $a^{m+1-k}b^k$ is obtained from multiplying $a^{m-k}b^k$ by a and $a^{m-(k-1)}b^{k-1}$ by b *[because* $m+1-k = m-(k-1)$*]*. Hence the coefficient of $a^{m+1-k}b^k$ equals the sum of $\binom{m}{k}$ and $\binom{m}{k-1}$. This is the crux of the algebraic proof.

If n and r are nonnegative integers and $r \le n$, then $\binom{n}{r}$ is called a **binomial coefficient** because it is one of the coefficients in the expansion of the binomial expression $(a+b)^n$.

The combinatorial proof of the binomial theorem follows.

Proof of Binomial Theorem (combinatorial version):

[The combinatorial argument used here to prove the binomial theorem works only for $n \ge 1$*. If we were giving only this combinatorial proof, we would have to prove the case* $n = 0$ *separately. Since we have already given a complete algebraic proof that includes the case* $n = 0$*, we do not prove it again here.]*

Let a and b be real numbers and n an integer that is at least 1. The expression $(a+b)^n$ can be expanded into products of n letters, where each letter is either a or b.

For each $k = 0, 1, 2, \ldots, n$, the product

$$a^{n-k}b^k = \underbrace{a \cdot a \cdot a \cdot \cdots a}_{n-k \text{ factors}} \cdot \underbrace{b \cdot b \cdot b \cdots b}_{k \text{ factors}}$$

occurs as a term in the sum the same number of times as there are orderings of $(n-k)$ a's and k b's. But this number equals $\binom{n}{k}$, the number of ways to choose k positions into which to place the b's. *[The other $n-k$ positions will be filled by a's.]* Hence, when like terms are combined, the coefficient of $a^{n-k}b^k$ in the sum is $\binom{n}{k}$. Thus

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k,$$

as was to be shown.

Example 9.7.5 **Substituting into the Binomial Theorem**

Expand the following expressions using the binomial theorem:

a. $(a+b)^5$ b. $(x-4y)^4$

Solution

a. $$\begin{aligned}(a+b)^5 &= \sum_{k=0}^{5} \binom{5}{k} a^{5-k}b^k \\ &= a^5 + \binom{5}{1}a^{5-1}b^1 + \binom{5}{2}a^{5-2}b^2 + \binom{5}{3}a^{5-3}b^3 + \binom{5}{4}a^{5-4}b^4 + b^5 \\ &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5\end{aligned}$$

b. Observe that $(x-4y)^4 = (x+(-4y))^4$. So let $a = x$ and $b = (-4y)$, and substitute into the binomial theorem.

$$\begin{aligned}(x-4y)^4 &= \sum_{k=0}^{4} \binom{4}{k} x^{4-k}(-4y)^k \\ &= x^4 + \binom{4}{1}x^{4-1}(-4y)^1 + \binom{4}{2}x^{4-2}(-4y)^2 + \binom{4}{3}x^{4-3}(-4y)^3 + (-4y)^4 \\ &= x^4 + 4x^3(-4y) + 6x^2(16y^2) + 4x^1(-64y^3) + (256y^4) \\ &= x^4 - 16x^3y + 96x^2y^2 - 256xy^3 + 256y^4\end{aligned}$$

■

Example 9.7.6 **Deriving Another Combinatorial Identity from the Binomial Theorem**

Use the binomial theorem to show that

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$$

for each integer $n \geq 0$.

Solution Since $2 = 1 + 1$, $2^n = (1 + 1)^n$. Apply the binomial theorem to this expression by letting $a = 1$ and $b = 1$. Then

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k} \cdot 1 \cdot 1$$

because $1^{n-k} = 1$ and $1^k = 1$. Consequently,

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}.$$

■

Example 9.7.7 **Using a Combinatorial Argument to Derive the Same Identity**

According to Theorem 6.3.1, a set with n elements has 2^n subsets. Apply this fact to give a combinatorial argument to justify the identity

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n.$$

Solution Suppose S is a set with n elements. Then every subset of S has some number of elements k, where k is between 0 and n. It follows that the total number of subsets of S, $N(\mathcal{P}(S))$, can be expressed as the following sum:

$$\begin{bmatrix}\text{the number}\\ \text{of subsets}\\ \text{of } S\end{bmatrix} = \begin{bmatrix}\text{the number}\\ \text{of subsets of}\\ \text{size 0}\end{bmatrix} + \begin{bmatrix}\text{the number}\\ \text{of subsets}\\ \text{of size 1}\end{bmatrix} + \cdots + \begin{bmatrix}\text{the number}\\ \text{of subsets}\\ \text{of size } n\end{bmatrix}$$

Now, for each integer k from 1 through n, the number of subsets of size k of a set with n elements is $\binom{n}{k}$. Hence the

$$\text{number of subsets of } S = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}.$$

By Theorem 6.3.1, S has 2^n subsets. Hence

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n.$$

■

Example 9.7.8 **Using the Binomial Theorem to Simplify a Sum**

Express the following sum in **closed form** (without using a summation symbol and without using an ellipsis $\cdots$):

$$\sum_{k=0}^{n} \binom{n}{k} 9^k.$$

Solution When the number 1 is raised to any power, the result is still 1. Thus

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} 9^k &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 9^k \\ &= (1 + 9)^n \quad \text{by the binomial theorem with } a = 1 \text{ and } b = 9 \\ &= 10^n.\end{aligned}$$

■

TEST YOURSELF

1. If n and r are nonnegative integers with $r \le n$, then the relation between $\binom{n}{r}$ and $\binom{n}{n-r}$ is _____.
2. Pascal's formula says that if n and r are positive integers with $r \le n$, then _____.
3. The crux of the algebraic proof of Pascal's formula is that to add two fractions you need to express both of them with a _____.
4. The crux of the combinatorial proof of Pascal's formula is that the set of subsets of size r of a set $\{x_1, x_2, \ldots, x_{n+1}\}$ can be partitioned into the set of subsets of size r that contain _____ and the set of subsets of size r that _____.
5. The binomial theorem says that given any real numbers a and b and any nonnegative integer n, _____.
6. The crux of the algebraic proof of the binomial theorem is that, after making a change of variable so that two summations have the same lower and upper limits and the exponents of a and b are the same, you use the fact that $\binom{m}{k} + \binom{m}{k-1} =$ _____.
7. The crux of the combinatorial proof of the binomial theorem is that the number of ways to arrange k b's and $(n-k)$ a's in a row is _____.

EXERCISE SET 9.7

In 1–4, use Theorem 9.5.1 to compute the values of the indicated quantities. (Assume n is an integer.)

1. $\binom{n}{0}$, for $n \ge 0$
2. $\binom{n}{1}$, for $n \ge 1$
3. $\binom{n}{2}$, for $n \ge 2$
4. $\binom{n}{3}$, for $n \ge 3$
5. Use Theorem 9.5.1 to prove algebraically that $\binom{n}{r} = \binom{n}{n-r}$, for integers n and r with $0 \le r \le n$. (This can be done by direct calculation; it is not necessary to use mathematical induction.)

Justify the equations in 6–9 either by deriving them from formulas in Example 9.7.1 or by direct computation from Theorem 9.5.1. Assume m, n, k, and r are integers.

6. $\binom{m+k}{m+k-1} = m + k$, for $m + k \ge 1$
7. $\binom{n+3}{n+1} = \dfrac{(n+3)(n+2)}{2}$, for $n \ge -1$
8. $\binom{k-r}{k-r} = 1$, for $k - r \ge 0$
9. $\binom{2(n+1)}{2n} = (n+1)(2n+1)$, for $n \ge 0$
10. **a.** Use Pascal's triangle given in Table 9.7.1 to compute the values of $\binom{6}{2}$, $\binom{6}{3}$, $\binom{6}{4}$, and $\binom{6}{5}$.
    b. Use the result of part (a) and Pascal's formula to compute $\binom{7}{3}$, $\binom{7}{4}$, and $\binom{7}{5}$.
    c. Complete the row of Pascal's triangle that corresponds to $n = 7$.
11. The row of Pascal's triangle that corresponds to $n = 8$ is as follows:

    1 8 28 56 70 56 28 8 1.

    What is the row that corresponds to $n = 9$?
12. Use Pascal's formula repeatedly to derive a formula for $\binom{n+3}{r}$ in terms of values of $\binom{n}{k}$ with $k \le r$. (Assume n and r are integers with $n \ge r \ge 3$.)
13. Use Pascal's formula to prove by mathematical induction that if n is an integer and $n \ge 1$, then

$$\sum_{i=2}^{n+1} \binom{i}{2} = \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n+1}{2} = \binom{n+2}{3}.$$

H 14. Prove that if n is an integer and $n \ge 1$, then

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = 2\binom{n+2}{3}.$$

15. Prove the following generalization of exercise 13: Let r be a fixed nonnegative integer. For every integer n with $n \ge r$,

$$\sum_{i=2}^{n} \binom{i}{r} = \binom{n+1}{r+1}.$$

16. Think of a set with $m + n$ elements as composed of two parts, one with m elements and the other with n elements. Give a combinatorial argument to show that

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{m}{r-1} + \cdots + \binom{m}{r}\binom{n}{0},$$

where m and n are positive integers and r is an integer that is less than or equal to both m and n. This identity gives rise to many useful additional

identities involving the quantities $\binom{n}{k}$. Because Alexander Vandermonde published an influential article about it in 1772, it is generally called the *Vandermonde convolution*. However, it was known at least in the 1300s in China by Chu Shih-chieh.

H 17. Prove that for every integer $n \geq 0$,

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

18. Let m be any nonnegative integer. Use mathematical induction and Pascal's formula to prove that for every integer $n \geq 0$,

$$\binom{m}{0} + \binom{m+1}{1} + \cdots + \binom{m+n}{n} = \binom{m+n+1}{n}.$$

Use the binomial theorem to expand the expressions in 19–27.

19. $(1+x)^7$ **20.** $(p+q)^6$ **21.** $(1-x)^6$

22. $(u-v)^5$ **23.** $(p-2q)^4$ **24.** $(u-3v)^4$

25. $\left(x+\frac{1}{x}\right)^5$ **26.** $\left(\frac{3}{a}-\frac{a}{3}\right)^5$ **27.** $\left(x^2+\frac{1}{x}\right)^5$

28. In Example 9.7.5 it was shown that

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

Evaluate $(a+b)^6$ by substituting the expression above into the equation

$$(a+b)^6 = (a+b)(a+b)^5$$

and then multiplying out and combining like terms.

In 29–34, find the coefficient of the given term when the expression is expanded by the binomial theorem.

29. x^6y^3 in $(x+y)^9$ **30.** x^7 in $(2x+3)^{10}$

31. a^5b^7 in $(a-2b)^{12}$ **32.** $u^{16}v^4$ in $(u^2-v^2)^{10}$

33. $p^{16}q^7$ in $(3p^2-2q)^{15}$ **34.** x^9y^{10} in $(2x-3y^2)^{14}$

35. As in the proof of the binomial theorem, transform the summation

$$\sum_{k=0}^{n} \binom{m}{k} a^{m-k}b^{k+1}$$

by making the change of variable $j = k+1$.

Use the binomial theorem to prove each statement in 36–41.

36. For every integer $n \geq 1$,

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0.$$

(*Hint:* Use the fact that $1 + (-1) = 0$.)

H 37. For every integer $n \geq 0$,

$$3^n = \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n}.$$

38. For every integer $m \geq 0$, $\displaystyle\sum_{i=0}^{m} (-1)^i \binom{m}{i} 2^{m-i} = 1$.

39. For every integer $n \geq 0$, $\displaystyle\sum_{i=0}^{n} (-1)^i \binom{n}{i} 3^{n-i} = 2^n$.

40. For every integer $n \geq 0$ and for every nonnegative real number x, $1 + nx \leq (1+x)^n$.

H 41. For every integer $n \geq 1$,

$$\binom{n}{0} - \frac{1}{2}\binom{n}{1} + \frac{1}{2^2}\binom{n}{2} - \frac{1}{2^3}\binom{n}{3} + \cdots + (-1)^{n-1}\frac{1}{2^{n-1}}\binom{n}{n-1} = \begin{cases} 0 & \text{if } n \text{ is even} \\ \dfrac{1}{2^{n-1}} & \text{if } n \text{ is odd.} \end{cases}$$

42. Use mathematical induction to prove that for every integer $n \geq 1$, if S is a set with n elements, then S has the same number of subsets with an even number of elements as with an odd number of elements. Use this fact to give a combinatorial argument to justify the identity of exercise 36.

Express each of the sums in 43–54 in closed form (without using a summation symbol and without using an ellipsis . . .).

43. $\displaystyle\sum_{k=0}^{n} \binom{n}{k} 5^k$ **44.** $\displaystyle\sum_{i=0}^{m} \binom{m}{i} 4^i$

45. $\displaystyle\sum_{i=0}^{n} \binom{n}{i} x^i$ **46.** $\displaystyle\sum_{k=0}^{n} \binom{m}{k} 2^{m-k}x^k$

47. $\displaystyle\sum_{j=0}^{2n} (-1)^j \binom{2n}{j} x^j$ **48.** $\displaystyle\sum_{r=0}^{n} \binom{n}{r} x^{2r}$

49. $\displaystyle\sum_{i=0}^{m} \binom{m}{i} p^{m-i}q^{2i}$ **50.** $\displaystyle\sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^k}$

51. $\displaystyle\sum_{i=0}^{m} (-1)^i \binom{m}{i} \frac{1}{2^i}$ **52.** $\displaystyle\sum_{k=0}^{n} \binom{n}{k} 3^{2n-2k}2^{2k}$

53. $\sum_{i=0}^{m}(-1)^i\binom{n}{i}5^{n-i}2^i$ **54.** $\sum_{k=0}^{n}(-1)^k\binom{n}{k}3^{2n-2k}2^{2k}$

* **55.** (For students who have studied calculus.)

a. Explain how the equation below follows from the binomial theorem:

$$(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^k.$$

b. Write the formula obtained by taking the derivative of both sides of the equation in part (a) with respect to x.

c. Use the result of part (b) to derive the formulas below.

(i) $2^{n-1}=\frac{1}{n}\left[\binom{n}{1}+2\binom{n}{2}+3\binom{n}{3}+\cdots+n\binom{n}{n}\right]$

(ii) $\sum_{k=0}^{n}k\binom{n}{k}(-1)^k=0$

d. Express $\sum_{k=1}^{n}k\binom{n}{k}3^k$ in closed form (without using a summation sign or ellipsis).

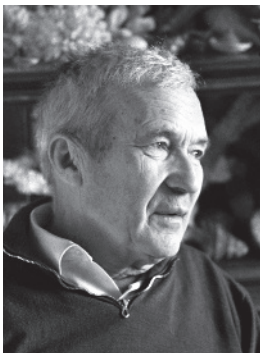
ANSWERS FOR TEST YOURSELF

1. $\binom{n}{r}=\binom{n}{n-r}$ **2.** $\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$ **3.** common denominator **4.** x_{n+1}; do not contain x_{n+1}

5. $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ **6.** $\binom{m+1}{k}$ **7.** $\binom{n}{k}$

9.8 Probability Axioms and Expected Value

The theory of probability is at bottom nothing but common sense reduced to a calculus. —Pierre-Simon Laplace (1749–1827)



ITAR-TASS News Agency/Alamy

Andrei Nikolaevich Kolmogorov (1903–1987)

Up to this point, we have calculated probabilities only for situations, such as tossing a fair coin or rolling a pair of balanced dice, where the outcomes in the sample space are all equally likely. But coins are not always fair and dice are not always balanced. How is it possible to calculate probabilities for these more general situations?

The following axioms were formulated by A. N. Kolmogorov in 1933 to provide a theoretical foundation for a far-ranging theory of probability. In this section we state the axioms, derive a few consequences, and introduce the notion of expected value.

Recall that a sample space is a set of all outcomes of a random process or experiment and that an event is a subset of a sample space.

Probability Axioms

Let S be a sample space. A **probability function** P from the set of all events in S to the set of real numbers satisfies the following three axioms: For all events A and B in S:

1. $0 \le P(A) \le 1$.
2. $P(\varnothing) = 0$ and $P(S) = 1$.
3. If A and B are disjoint (that is, if $A \cap B = \varnothing$), then the probability of the union of A and B is

$$P(A \cup B) = P(A) + P(B).$$

Example 9.8.1 **Applying the Probability Axioms**

Suppose that A and B are events in a sample space S. If A and B are disjoint, could $P(A) = 0.6$ and $P(B) = 0.8$?

Solution No. Probability axiom 3 would imply that $P(A \cup B) = P(A) + P(B) = 0.6 + 0.8 = 1.4$, and since $1.4 > 1$, this result would violate probability axiom 1. ■

Example 9.8.2 **The Probability of the Complement of an Event**

Suppose that A is an event in a sample space S. Deduce that $P(A^c) = 1 - P(A)$.

Solution By Theorem 6.2.2(5), with S representing the universal set U,

$$A \cap A^c = \varnothing \quad \text{and} \quad A \cup A^c = S.$$

Thus S is the disjoint union of A and A^c, and so

$$P(A \cup A^c) = P(A) + P(A^c) = P(S) = 1.$$

So $P(A) + P(A^c) = 1$ and subtracting $P(A)$ from both sides gives the result that $P(A^c) = 1 - P(A)$. ■

Probability of the Complement of an Event

If A is any event in a sample space S, then

$$P(A^c) = 1 - P(A). \qquad 9.8.1$$

It is important to check that Kolmogorov's probability axioms are consistent with the results obtained using the equally likely probability formula. To see that this is the case, let S be a finite sample space with outcomes $a_1, a_2, a_3, \ldots, a_n$. It is clear that all the singleton sets $\{a_1\}, \{a_2\}, \{a_3\}, \ldots, \{a_n\}$ are mutually disjoint and that their union is S. Since $P(S) = 1$, probability axiom 3 can be applied multiple times (see exercise 13 at the end of this section) to obtain

$$P(\{a_1\} \cup \{a_2\} \cup \{a_3\} \cup \cdots \cup \{a_n\}) = \sum_{k=1}^{n} P(\{a_k\}) = 1.$$

If, in addition, all the outcomes are equally likely, there is a positive real number c so that

$$P(\{a_1\}) = P(\{a_2\}) = P(\{a_3\}) = \cdots = P(\{a_n\}) = c.$$

Hence

$$1 = \sum_{k=1}^{n} c = \underbrace{c + c + \cdots + c}_{n \text{ terms}} = nc,$$

and thus

$$c = \frac{1}{n}.$$

It follows that if A is any event with outcomes $a_{i_1}, a_{i_2}, a_{i_3}, \ldots, a_{i_m}$, then

$$P(A) = \sum_{k=1}^{m} P(\{a_{i_k}\}) = \sum_{k=1}^{m} \frac{1}{n} = \frac{m}{n} = \frac{N(A)}{N(S)},$$

which is the result given by the equally likely probability formula.

Example 9.8.3 **The Probability of a General Union of Two Events**

Follow the steps outlined in parts (a) and (b) below to prove the following formula:

Probability of a General Union of Two Events

If S is any sample space and A and B are any events in S, then

$$P(A \cup B) = P(A) + P(B) - P(A \cap B). \qquad 9.8.2$$

In both steps, suppose that A and B are any events in a sample space S.

a. Show that $A \cup B$ is a disjoint union of the following sets: $A - (A \cap B)$, $B - (A \cap B)$, and $A \cap B$.

b. For any events U and V in a sample space S, if $U \subseteq V$ then $P(V - U) = P(V) - P(U)$. Use this result (which you are asked to prove in exercise 12 at the end of this section) and the result of part (a) to finish the proof of the formula.

Solution

a. Refer to Figure 9.8.1 as you read the following explanation. Elements in the set $A - (A \cap B)$ are in the region shaded blue, elements in $B - (A \cap B)$ are in the region shaded gray, and elements in $A \cap B$ are in the white region.

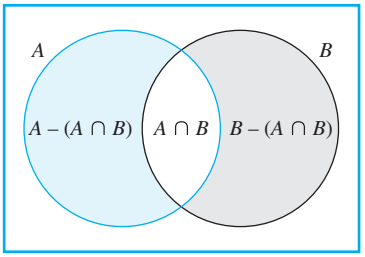


FIGURE 9.8.1

Part 1: Show that $A \cup B \subseteq (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$***:*** Given any element x in $A \cup B$, x satisfies exactly one of the following three conditions:

(1) $x \in A$ and $x \in B$

(2) $x \in A$ and $x \notin B$

(3) $x \in B$ and $x \notin A$.

1. In the first case, $x \in A \cap B$, and so $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ by definition of union.
2. In the second case, $x \notin A \cap B$ (because $x \notin B$), and so $x \in A - (A \cap B)$. Therefore $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ by definition of union.
3. In the third case, $x \notin A \cap B$ (because $x \notin A$), and hence $x \in B - (A \cap B)$. So, again, $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ by definition of union.

Hence, in all three cases, $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$, which completes the proof of part 1.

Moreover, since the three conditions are mutually exclusive, the three sets $A - (A \cap B)$, $B - (A \cap B)$, and $A \cap B$ are mutually disjoint.

Part 2: Show that $(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B) \subseteq A \cup B$***:*** Suppose x is any element in $(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$. By definition of union, $x \in A - (A \cap B)$ or $x \in B - (A \cap B)$ or $x \in A \cap B$.

1. In the first case, $x \in A - (A \cap B)$, and so $x \in A$ and $x \notin A \cap B$ by definition of set difference. In particular, $x \in A$ and thus $x \in A \cup B$.
2. In the second case, $x \in B - (A \cap B)$, and so $x \in B$ and $x \notin A \cap B$ by definition of set difference. In particular, $x \in B$ and thus $x \in A \cup B$.
3. In the third case, $x \in A \cap B$, and so, in particular, $x \in A$. Thus $x \in A \cup B$.

Hence, in all three cases, $x \in A \cup B$, which completes the proof of part 2.

b. $P(A \cup B) = P((A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B))$ by part (a)
$= P(A - (A \cap B)) + P(B - (A \cap B)) + P(A \cap \mathrm{B})$
by exercise 13 at the end of the section and the fact that $A - (A \cap B)$, $B - (A \cap B)$, and $A \cap B$ are mutually disjoint
$= P(A) - P(A \cap B) + P(B) - P(A \cap B) + P(A \cap B)$
by exercise 12 at the end of the section because $A \cap B \subseteq A$ and $A \cap B \subseteq B$
$= P(A) + P(B) - P(A \cap B)$ by algebra. ■

Example 9.8.4 **Computing the Probability of a General Union of Two Events**

Suppose a card is chosen at random from an ordinary 52-card deck (see Section 9.1). What is the probability that the card is a face card (jack, queen, or king) or is from one of the red suits (hearts or diamonds)?

Solution Let A be the event that the chosen card is a face card, and let B be the event that the chosen card is from one of the red suits. The event that the card is a face card or is from one of the red suits is $A \cup B$. Now $N(A) = 4 \cdot 3 = 12$ (because each of the four suits has three face cards), and so $P(A) = 12/52$. Also $N(B) = 26$ (because half the cards are red), and so $P(B) = 26/52$. Finally, $N(A \cap B) = 6$ (because there are three face cards in hearts and another three in diamonds), and so $P(A \cap B) = 6/52$. It follows from the formula for the probability of a union of any two events that

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{12}{52} + \frac{26}{52} - \frac{6}{52} = \frac{32}{52} \cong 61.5\%.$$

Thus the probability that the chosen card is a face card or is from one of the red suits is approximately 61.5%. ■

Expected Value

People who regularly buy lottery tickets often justify the practice by saying that, even though they know that on average they will lose money, they are hoping for one significant gain, after which they believe they will quit playing. Unfortunately, when people who have lost money on a string of losing lottery tickets win some or all of it back, they generally decide to keep trying their luck instead of quitting.

The technical way to say that on average a person will lose money on the lottery is to say that the *expected value* of playing the lottery is negative.

Definition

Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, a_3, \ldots, a_n$, which occur with probabilities $p_1, p_2, p_3, \ldots, p_n$. The **expected value** of the process is

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + a_n p_n.$$

Example 9.8.5 **Expected Value of a Lottery**

Suppose that 500,000 people pay \$5 each to play a lottery game with the following prizes: one grand prize of \$1,000,000, 10 second prizes of \$1,000 each, 1,000 third prizes of \$500 each, and 10,000 fourth prizes of \$10 each. What is the expected value of a ticket?

Solution Each of the 500,000 lottery tickets has the same chance as any other of containing a winning lottery number, and so $p_k = \frac{1}{500{,}000}$ for each $k = 1, 2, 3, \ldots, 500{,}000$. Let a_i be the net gain for an individual ticket a_i, where $a_1 = 999{,}995$ (the net gain for the grand-prize ticket, which is one million dollars minus the \$5 cost of the winning ticket), $a_2 = a_3 = \cdots = a_{11} = 995$ (the net gain for each of the 10 second-prize tickets), $a_{12} = a_{13} = \cdots = a_{1{,}011} = 495$ (the net gain for each of the 1,000 third-prize tickets), and $a_{1{,}012} = a_{1{,}013} = \cdots = a_{11{,}011} = 5$ (the net gain for each of the 10,000 fourth-prize tickets). Since the remaining 488,989 tickets just lose \$5, $a_{11{,}012} = a_{11{,}013} = \cdots = a_{500{,}000} = -5$.

The expected value of a ticket is therefore

$$\sum_{k=1}^{500{,}000} a_k p_k = \sum_{k=1}^{500{,}000} \left(a_k \cdot \frac{1}{500{,}000} \right) \quad \text{because each } p_k = 1/500{,}000$$

$$= \frac{1}{500{,}000} \sum_{k=1}^{500{,}000} a_k \quad \text{by theorem 5.1.1(2)}$$

$$= \frac{1}{500{,}000}(999{,}995 + 10 \cdot 995 + 1{,}000 \cdot 495 + 10{,}000 \cdot 5 + (-5) \cdot 488{,}989)$$

$$= \frac{1}{500{,}000}(999{,}995 + 9{,}950 + 495{,}000 + 50{,}000 - 2{,}444{,}945)$$

$$= -1.78.$$

In other words, a person who continues to play this lottery for a very long time will probably win some money occasionally but on average will lose \$1.78 per ticket. ■

Example 9.8.6 **Gambler's Ruin**

A gambler repeatedly bets \$1 that a coin will come up heads when tossed. Each time the coin comes up heads, the gambler wins \$1; each time it comes up tails, he loses \$1. The gambler will quit playing either when he is ruined (loses all his money) or when he has \$$M$ (where M is a positive number he has decided in advance). Let P_n be the probability that the gambler is ruined if he begins playing with \$$n$. Then, if the coin is fair (has an equal chance of coming up heads or tails),

$$P_{k-1} = \frac{1}{2}P_k + \frac{1}{2}P_{k-2} \quad \text{for each integer } k \text{ with } 2 \le k \le M.$$

(This follows from the fact that if the gambler has \$$(k-1)$, then he has an equal chance of winning \$1 or losing \$1. If he wins \$1 then his chance of being ruined is P_k, whereas if he loses \$1 then his chance of being ruined is P_{k-2}.) Also $P_0 = 1$ (because if he has \$0, he is certain of being ruined) and $P_M = 0$ (because once he has \$$M$, he quits and so stands no chance of being ruined). Find an explicit formula for P_n. How should the gambler choose M to minimize his chance of being ruined?

Solution Multiplying both sides of $P_{k-1} = \frac{1}{2}P_k + \frac{1}{2}P_{k-2}$ by 2 and subtracting P_{k-2} from both sides gives

$$P_k = 2P_{k-1} - P_{k-2}.$$

This is a second-order homogeneous recurrence relation with constant coefficients. Because $P_k - 2P_{k-1} + P_{k-2} = 0$, its characteristic equation is

$$t^2 - 2t + 1 = 0,$$

which has the single root $r = 1$. Thus, by the single-root theorem from Section 5.8,

$$P_n = Cr^n + Dnr^n = C + Dn$$

(since $r = 1$), where C and D are determined by two values of the sequence. Since $P_0 = 1$ and $P_M = 0$,

$$1 = P_0 = C + D \cdot 0 = C$$
$$0 = P_M = C + D \cdot M = 1 + D \cdot M.$$

It follows that $C = 1$ and $D = -\frac{1}{M}$, and so

$$P_n = 1 - \frac{1}{M}n = \frac{M-n}{M} \quad \text{for each integer } n \text{ with } 0 \le n \le M.$$

For instance, a gambler who starts with \$20 and decides to quit either if his total grows to \$100 or if he goes broke has the following chance of going broke:

$$P_{20} = \frac{100-20}{100} = \frac{80}{100} = 80\%.$$

Observe that the larger M is relative to n, the closer P_n is to 1. In other words, the larger the amount of money the gambler sets himself as a target, the more likely he is to go broke. Conversely, the more modest he is in his goal, the more likely he is to reach it. ■

TEST YOURSELF

1. If A is an event in a sample space S, $P(A)$ can take values between _____ and _____. Moreover, $P(S) =$ _____ and $P(\varnothing) =$ _____.
2. If A and B are disjoint events in a sample space S, $P(A \cup B) =$ _____.
3. If A is an event in a sample space S, $P(A^c) =$ _____.
4. If A and B are any events in a sample space S, $P(A \cup B) =$ _____.
5. If the possible outcomes of a random process or experiment are real numbers $a_1, a_2, \ldots, a_n$, which occur with probabilities $p_1, p_2, \ldots, p_n$, then the expected value of the process is _____.

EXERCISE SET 9.8

1. In any sample space S, what is $P(\varnothing)$?
2. Suppose A, B, and C are mutually exclusive events in a sample space S, $A \cup B \cup C = S$, and A and B have probabilities 0.3 and 0.5, respectively.
   a. What is $P(A \cup B)$? **b.** What is $P(C)$?
3. Suppose A and B are mutually exclusive events in a sample space S, C is another event in S, $A \cup B \cup C = S$, and A and B have probabilities 0.4 and 0.2, respectively.
   a. What is $P(A \cup B)$?
   b. Is it possible that $P(C) = 0.2$? Explain.
4. Suppose A and B are events in a sample space S with probabilities 0.8 and 0.7, respectively. Suppose also that $P(A \cap B) = 0.6$. What is $P(A \cup B)$?
5. Suppose A and B are events in a sample space S and suppose that $P(A) = 0.6$, $P(B^c) = 0.4$, and $P(A \cap B) = 0.2$. What is $P(A \cup B)$?
6. Suppose U and V are events in a sample space S and suppose that $P(U^c) = 0.3$, $P(V) = 0.6$, and $P(U^c \cup V^c) = 0.4$. What is $P(U \cup V)$?
7. Suppose a sample space S consists of three outcomes: 0, 1, and 2. Let $A = \{0\}$, $B = \{1\}$, and $C = \{2\}$, and suppose $P(A) = 0.4$ and $P(B) = 0.3$. Find each of the following:
   a. $P(A \cup B)$
   b. $P(C)$
   c. $P(A \cup C)$
   d. $P(A^c)$

e. $P(A^c \cap B^c)$
f. $P(A^c \cup B^c)$

8. Redo exercise 7 assuming that $P(A) = 0.5$ and $P(B) = 0.4$.

9. Let A and B be events in a sample space S, and let $C = S - (A \cup B)$. Suppose $P(A) = 0.4$, $P(B) = 0.5$, and $P(A \cap B) = 0.2$. Find each of the following:
a. $P(A \cup B)$
b. $P(C)$
c. $P(A^c)$
d. $P(A^c \cap B^c)$
e. $P(A^c \cup B^c)$
f. $P(B^c \cap C)$

10. Redo exercise 9 assuming that $P(A) = 0.7$, $P(B) = 0.3$, and $P(A \cap B) = 0.1$.

***H* 11.** Prove that if S is any sample space and U and V are events in S with $U \subseteq V$, then $P(U) \leq P(V)$.

***H* 12.** Prove that if S is any sample space and U and V are any events in S, then $P(V - U) = P(V) - P(U \cap V)$.

***H* 13.** Use the axioms for probability and mathematical induction to prove that for each integer $n \geq 2$, if $A_1, A_2, A_3, \ldots, A_n$ are any mutually disjoint events in a sample space S, then

$$P(A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n) = \sum_{k=1}^{n} P(A_k).$$

14. A lottery game offers \$2 million to the grand prize winner, \$20 to each of 10,000 second prize winners, and \$4 to each of 50,000 third prize winners. The cost of the lottery is \$2 per ticket. Suppose that 1.5 million tickets are sold. What is the expected gain or loss of a ticket?

15. A company offers a raffle whose grand prize is a \$40,000 new car. Additional prizes are a \$1,000 television and a \$500 computer. Tickets cost \$20 each. Ticket income over the cost of the prizes will be donated to charity. If 3,000 tickets are sold, what is the expected gain or loss of each ticket?

16. An urn contains four balls numbered 2, 2, 5, and 6. If a person selects a set of two balls at random, what is the expected value of the sum of the numbers on the balls?

17. An urn contains five balls numbered 1, 2, 2, 8, and 8. If a person selects a set of two balls at random, what is the expected value of the sum of the numbers on the balls?

18. An urn contains five balls numbered 1, 2, 2, 8, and 8. If a person selects a set of three balls at random, what is the expected value of the sum of the numbers on the balls?

19. When a pair of balanced dice are rolled and the sum of the numbers showing face up is computed, the result can be any number from 2 to 12, inclusive. What is the expected value of the sum?

***H* 20.** Suppose a person offers to play a game with you. In this game, when you draw a card from a standard 52-card deck, if the card is a face card you win \$3, and if the card is anything else you lose \$1. If you agree to play the game, what is your expected gain or loss?

21. A person pays \$1 to play the following game: The person tosses a fair coin four times. If no heads occur, the person pays an additional \$2, if one head occurs, the person pays an additional \$1, if two heads occur, the person just loses the initial dollar, if three heads occur, the person wins \$3, and if four heads occur, the person wins \$4. What is the person's expected gain or loss?

***H* 22.** A fair coin is tossed until either a head comes up or four tails are obtained. What is the expected number of tosses?

***H* 23.** A gambler repeatedly bets that a die will come up 6 when rolled. Each time the die comes up 6, the gambler wins \$1; each time it does not, the gambler loses \$1. He will quit playing either when he is ruined or when he wins \$300. If P_n is the probability that the gambler is ruined when he begins play with \$$n$, then $P_{k-1} = \frac{1}{6}P_k + \frac{5}{6}P_{k-2}$ for every integer k with $2 \leq k \leq 300$. Also $P_0 = 1$ and $P_{300} = 0$. Find an explicit formula for P_n and use it to calculate P_{20}. (Exercise 33 in Section 9.9 asks you to derive the recurrence relation for this sequence.)

ANSWERS FOR TEST YOURSELF

1. 0; 1; 1; 0 **2.** $P(A) + P(B)$ **3.** $1 - P(A)$ **4.** $P(A) + P(B) - P(A \cap B)$ **5.** $a_1p_1 + a_2p_2 + \cdots + a_np_n$

9.9 Conditional Probability, Bayes' Formula, and Independent Events

It is remarkable that a science which began with the consideration of games of chance should have become the most important object of human knowledge.... The most important questions of life are, for the most part, really only problems of probability. —Pierre-Simon Laplace, 1749–1827

In this section we introduce the notion of conditional probability and discuss Bayes' theorem and the kind of interesting results to which it leads. We then define the concept of independent events and give some applications.

Conditional Probability

Imagine a couple with two children, each of whom is equally likely to be a boy or a girl. Now suppose you are given the information that one is a boy. What is the probability that the other child is a boy?

Figure 9.9.1 shows four equally likely combinations of gender for the children. You can imagine that the first letter refers to the older child and the second letter to the younger. Thus the combination *BG* indicates that the older child is a boy and the younger is a girl.

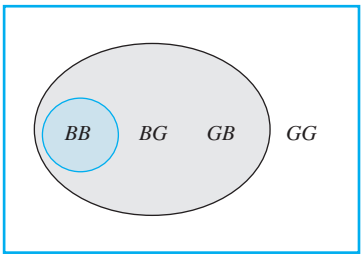


FIGURE 9.9.1

There are three combinations where one of the children is a boy, and in one of these three combinations the other child is also a boy. Given that you know one child is a boy, only these three combinations could be the case. So you can think of the set of those outcomes as a new sample space with three elements, all of which are equally likely. Within the new sample space, there is one combination where the other child is a boy. Thus it would be reasonable to say that the likelihood that the other child is a boy, given that at least one is a boy, is $1/3 = 33\frac{1}{3}\%$. Given that the original sample space contained four outcomes note that the following computation gives the same result:

$$\frac{P(\text{at least one child is a boy and the other child is also a boy})}{P(\text{at least one child is a boy})} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}.$$

A generalization of this observation forms the basis for the following definition.

Definition

Let A and B be events in a sample space S. If $P(A) \neq 0$, then the **conditional probability of B given A**, denoted $\boldsymbol{P(B|A)}$, is

$$P(B|A) = \frac{P(A \cap B)}{P(A)}. \qquad 9.9.1$$

Example 9.9.1 **Computing a Conditional Probability**

A pair of fair dice, one blue and the other gray, are rolled. What is the probability that the sum of the numbers showing face up is 8, given that both of the numbers are even?

Solution The sample space is the set of all 36 outcomes obtained from rolling the two dice and noting the numbers showing face up on each. As in Section 9.1, denote by ab the outcome that the number showing face up on the blue die is a and the one on the gray die is b. Let A be the event that both numbers are even and B the event that the sum of the numbers is 8. Then $A = \{22, 24, 26, 42, 44, 46, 62, 64, 66\}$, $B = \{26, 35, 44, 53, 62\}$, and $A \cap B = \{26, 44, 62\}$. Because the dice are fair (so all outcomes are equally likely), $P(A) = 9/36$, $P(B) = 5/36$, and $P(A \cap B) = 3/36$. By definition of conditional probability,

$$P(B|A) = \frac{P(A \cap \mathrm{B})}{P(A)} = \frac{\frac{3}{36}}{\frac{9}{36}} = \frac{3}{9} = \frac{1}{3}.$$ ■

Note that when both sides of the formula for conditional probability (formula 9.9.1) are multiplied by $P(A)$, a formula for $P(A \cap B)$ is obtained:

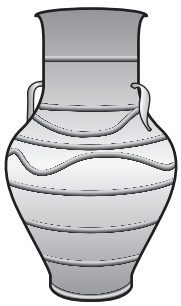
$$P(A \cap B) = P(B|A) \cdot P(A). \qquad 9.9.2$$

And dividing both sides of formula (9.9.2) by $P(B|A)$ gives a formula for $P(A)$:

$$P(A) = \frac{P(A \cap B)}{P(B|A)}. \qquad 9.9.3$$

Example 9.9.2 **Representing Conditional Probabilities with a Tree Diagram**

An urn contains 5 blue and 7 gray balls. Let us say that 2 are chosen at random, one after the other, without replacement.



a. Find the following probabilities and illustrate them with a tree diagram: the probability that both balls are blue, the probability that the first ball is blue and the second is not blue, the probability that the first ball is not blue and the second ball is blue, and the probability that neither ball is blue.

b. What is the probability that the second ball is blue?

c. What is the probability that at least one of the balls is blue?

d. If the experiment of choosing two balls from the urn is repeated many times over, what is the expected value of the number of blue balls?

Solution Let S denote the sample space of all possible choices of two balls from the urn, let B_1 be the event that the first ball is blue, and let B_2 be the event that the second ball is blue. Then B_1^c is the event that the first ball is not blue and B_2^c is the event that the second ball is not blue.

a. Because there are 12 balls of which 5 are blue and 7 are gray, the probability that the first ball is blue is

$$P(B_1) = \frac{5}{12}$$

and the probability that the first ball is not blue is

$$P(B_1^c) = \frac{7}{12}.$$

If the first ball is blue, then the urn would contain 4 blue balls and 7 gray balls, and so

$$P(B_2|B_1) = \frac{4}{11} \quad \text{and} \quad P(B_2^c|B_1) = \frac{7}{11},$$

where $P(B_2|B_1)$ is the probability that the second ball is blue given that the first ball is blue and $P(B_2^c|B_1)$ is the probability that the second ball is not blue given that the first ball is blue. It follows from formula (9.9.2) that the probability that both balls are blue is

$$P(B_1 \cap B_2) = P(B_2|B_1) \cdot P(B_1) = \frac{4}{11} \cdot \frac{5}{12} = \frac{20}{132}.$$

And the probability that the first ball is blue and the second ball is not blue is

$$P(B_1 \cap B_2^c) = P(B_2^c|B_1) \cdot P(B_1) = \frac{7}{11} \cdot \frac{5}{12} = \frac{35}{132}.$$

Similarly, if the first ball is not blue, then the urn would contain 5 blue balls and 6 gray balls, and so

$$P(B_2|B_1^c) = \frac{5}{11} \quad \text{and} \quad P(B_2^c|B_1^c) = \frac{6}{11},$$

where $P(B_2|B_1^c)$ is the probability that the second ball is blue given that the first ball is not blue and $P(B_2^c|B_1^c)$ is the probability that the second ball is not blue given that the first ball is not blue. It follows from formula (9.9.2) that the probability that the first ball is not blue but the second ball is blue is

$$P(B_1^c \cap B_2) = P(B_2|B_1^c) \cdot P(B_1^c) = \frac{5}{11} \cdot \frac{7}{12} = \frac{35}{132}.$$

And the probability that neither the first ball nor the second ball is blue is

$$P(B_1^c \cap B_2^c) = P(B_2^c|B_1^c) \cdot P(B_1^c) = \frac{6}{11} \cdot \frac{7}{12} = \frac{42}{132}.$$

The tree diagram in Figure 9.9.2 is a convenient way to help calculate these results.

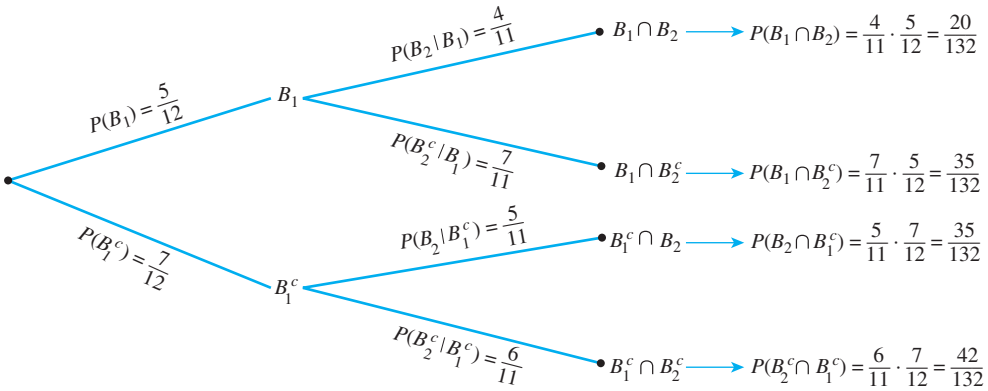


FIGURE 9.9.2

b. The event that the second ball is blue can occur in one of two mutually exclusive ways: Either the first ball is blue and the second is also blue, or the first ball is gray (not blue) and the second is blue.

In other words, B_2 is the disjoint union of $B_2 \cap B_1$ and $B_2 \cap B_1^c$. Hence

$$\begin{aligned} P(B_2) &= P((B_2 \cap B_1) \cup (B_2 \cap B_1^c)) \\ &= P(B_2 \cap B_1) + P(B_2 \cap B_1^c) \quad \text{by probability axiom 3} \\ &= \frac{20}{132} + \frac{35}{132} \quad \text{by part (a)} \\ &= \frac{55}{132} = \frac{5}{12}. \end{aligned}$$

Thus the probability that the second ball is blue is $5/12$, the same as the probability that the first ball is blue.

c. By formula 9.8.2, for the union of any two events,

$$\begin{aligned} P(B_1 \cup B_2) &= P(B_1) + P(B_2) - P(B_1 \cap B_2) \\ &= \frac{5}{12} + \frac{5}{12} - \frac{20}{132} \quad \text{by parts (a) and (b)} \\ &= \frac{90}{132} = \frac{15}{22}. \end{aligned}$$

Thus the probability is $15/22$, or approximately 68.2%, that at least one of the balls is blue.

d. The event that neither ball is blue is the complement of the event that at least one of the balls is blue, and so

$$\begin{aligned} P(0 \text{ blue balls}) &= 1 - P(\text{at least one ball is blue}) \quad \text{by formula 9.8.1} \\ &= 1 - \frac{15}{22} \quad \text{by part (c)} \\ &= \frac{7}{22}. \end{aligned}$$

The event that one ball is blue can occur in one of two mutually exclusive ways: Either the second ball is blue and the first is not, or the first ball is blue and the second is not. Part (a) showed that the probability of the first way is $\frac{35}{132}$, and the probability of the second way is also $\frac{35}{132}$. Thus, by probability axiom 3,

$$P(1 \text{ blue ball}) = \frac{35}{132} + \frac{35}{132} = \frac{70}{132}.$$

Finally, by part (a),

$$P(2 \text{ blue balls}) = \frac{20}{132}.$$

Therefore,

$$\begin{aligned} \begin{bmatrix} \text{the expected value} \\ \text{of the number} \\ \text{of blue balls} \end{bmatrix} &= 0 \cdot P(0 \text{ blue balls}) + 1 \cdot P(1 \text{ blue ball}) + 2 \cdot P(2 \text{ blue balls}) \\ &= 0 \cdot \frac{7}{22} + 1 \cdot \frac{70}{132} + 2 \cdot \frac{20}{132} \\ &= \frac{110}{132} \cong 0.8. \end{aligned}$$

■

Bayes' Theorem

Suppose that one urn contains 3 blue and 4 gray balls and a second urn contains 5 blue and 3 gray balls. A ball is selected by choosing one of the urns at random and then picking a ball at random from that urn. If the chosen ball is blue, what is the probability that it came from the first urn?

This problem can be solved by carefully interpreting all the information that is known and putting it together in just the right way. Let A be the event that the chosen ball is blue, B_1 the event that the ball came from the first urn, and B_2 the event that the ball came from the second urn. Because 3 of the 7 balls in urn one are blue, and 5 of the 8 balls in urn two are blue,

$$P(A|B_1) = \frac{3}{7} \quad \text{and} \quad P(A|B_2) = \frac{5}{8}.$$

And because the urns are equally likely to be chosen,

$$P(B_1) = P(B_2) = \frac{1}{2}.$$

Moreover, by formula (9.9.2),

$$P(A \cap B_1) = P(A|B_1) \cdot P(B_1) = \frac{3}{7} \cdot \frac{1}{2} = \frac{3}{14} \quad \text{and}$$
$$P(A \cap B_2) = P(A|B_2) \cdot P(B_2) = \frac{5}{8} \cdot \frac{1}{2} = \frac{5}{16}.$$

Now A is the disjoint union of $(A \cap B_1)$ and $(A \cap B_2)$, and so by probability axiom 3,

$$P(A) = P((A \cap B_1) \cup (A \cap B_2)) = P(A \cap B_1) + P(A \cap B_2) = \frac{3}{14} + \frac{5}{16} = \frac{59}{112}.$$

Finally, by definition of conditional probability,

$$P(B_1|A) = \frac{P(B_1 \cap A)}{P(A)} = \frac{\frac{3}{14}}{\frac{59}{112}} = \frac{336}{826} \cong 40.7\%.$$

Thus, if the chosen ball is blue, the probability is approximately 40.7% that it came from the first urn.

The steps used to derive the answer in the previous example can be generalized to prove Bayes' theorem. (See exercises 9 and 10 at the end of this section.) Thomas Bayes was an English Presbyterian minister who devoted much of his energies to mathematics. The theorem that bears his name was published posthumously in 1763. The portrait at the left is the only one attributed to him, but its authenticity has recently come into question.

Stephen M. Stigler

Thomas Bayes (1702–1761)

Theorem 9.9.1 Bayes' Theorem

Suppose a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, \ldots, B_n$, suppose A is an event in S, and suppose both A and each B_k have nonzero probabilities for every integer k with $1 \le k \le n$. Then

$$P(B_k|A) = \frac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots + P(A|B_n)P(B_n)}.$$

Example 9.9.3 **Applying Bayes' Theorem**

Most medical tests occasionally produce incorrect results, called false positives and false negatives. When a test is designed to determine whether a patient has a certain disease, a **false positive** result indicates that a patient has the disease when the patient does not have it. A **false negative** result indicates that a patient does not have the disease when the patient does have it.

When large-scale health screenings are performed for diseases with relatively low incidence, those who develop the screening procedures have to balance several considerations: the per-person cost of the screening, follow-up costs for further testing of false positives, and the possibility that people who have the disease will develop unwarranted confidence in the state of their health.

Consider a medical test that screens for a disease found in 5 people in 1,000. Suppose that the false positive rate is 3% and the false negative rate is 1%. Then 99% of the time a person who has the condition tests positive for it, and 97% of the time a person who does not have the condition tests negative for it. (See exercise 4 at the end of this section.)

a. What is the probability that a randomly chosen person who tests positive for the disease actually has the disease?

b. What is the probability that a randomly chosen person who tests negative for the disease does not in fact have the disease?

Solution Consider a person chosen at random from among those screened. Let A be the event that the person tests positive for the disease, B_1 the event that the person actually has the disease, and B_2 the event that the person does not have the disease. Then

$$P(A|B_1) = 0.99, \quad P(A^c|B_1) = 0.01, \quad P(A^c|B_2) = 0.97, \quad \text{and} \quad P(A|B_2) = 0.03.$$

Also, because 5 people in 1,000 have the disease,

$$P(B_1) = 0.005 \quad \text{and} \quad P(B_2) = 0.995.$$

a. By Bayes' theorem,

$$\begin{aligned} P(B_1|A) &= \frac{P(A|B_1)P(B_1)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2)} \\ &= \frac{(0.99)(0.005)}{(0.99)(0.005) + (0.03)(0.995)} \\ &\cong 0.1422 \cong 14.2\%. \end{aligned}$$

Thus the probability that a person with a positive test result actually has the disease is approximately 14.2%.

b. By Bayes' theorem,

$$\begin{aligned} P(B_2|A^c) &= \frac{P(A^c|B_2)P(B_2)}{P(A^c|B_1)P(B_1) + P(A^c|B_2)P(B_2)} \\ &= \frac{(0.97)(0.995)}{(0.01)(0.005) + (0.97)(0.995)} \\ &\cong 0.999948 \cong 99.995\%. \end{aligned}$$

Thus the probability that a person with a negative test result does not have the disease is approximately 99.995%.

You might be surprised by these numbers, but they are fairly typical of the situation where the screening test is significantly less expensive than a more accurate test for the

same disease yet produces positive results for nearly all people with the disease. Using the screening test limits the expense of unnecessarily using the more costly test to a relatively small percentage of the population being screened, while only rarely indicating that a person who has the disease is free of it. ■

Independent Events

Suppose a fair coin is tossed twice. It seems intuitively clear that the outcome of the first toss does not depend in any way on the outcome of the second toss, and conversely, the outcome of the second toss does not depend on the outcome of the first toss. In other words, if, for instance, A is the event that a head is obtained on the first toss and B is the event that a head is obtained on the second toss, then if the coin is tossed randomly both times, events A and B should be *independent* in the sense that $P(A|B) = P(A)$ and $P(B|A) = P(B)$. This intuitive idea of independence is supported by the following analysis. If the coin is fair, then the four outcomes HH, HT, TH, and TT are equally likely, and

$$A = \{HH, HT\}, \quad B = \{TH, HH\}, \quad A \cap B = \{HH\}.$$

Hence

$$P(A) = P(B) = \frac{2}{4} = \frac{1}{2}.$$

But also

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2} \quad \text{and} \quad P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2},$$

and thus $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

To obtain more convenient form for the definition of independence, observe that

$$\text{if } P(B) \neq 0 \text{ and } P(A|B) = P(A), \text{ then } P(A \cap B) = P(A|B) \cdot P(B) = P(A) \cdot P(B).$$

By the same argument,

$$\text{if } P(A) \neq 0 \text{ and } P(B|A) = P(B) \text{ then } P(A \cap B) = P(A) \cdot P(B).$$

Conversely (see exercise 18 at the end of this section),

$$\text{if } P(A \cap B) = P(A) \cdot P(B) \text{ and } P(A) \neq 0 \text{ then } P(B|A) = P(B)$$

and

$$\text{if } P(A \cap B) = P(A) \cdot P(B) \text{ and } P(B) \neq 0 \text{ then } P(A|B) = P(A).$$

Note It would be natural to think that mutually disjoint events would be independent, but in fact almost the opposite is true: Mutually disjoint events with nonzero probabilities are dependent.

Thus, we can eliminate the requirement that the probabilities be nonzero if we use the following product formula to define independent events.

Definition

If A and B are events in a sample space S, then A and B are **independent** if, and only if,

$$P(A \cap B) = P(A) \cdot P(B).$$

Example 9.9.4 **Disjoint Events and Independence**

Let A and B be events in a sample space S, and suppose $A \cap B = \varnothing$, $P(A) \neq 0$, and $P(B) \neq 0$. Show that $P(A \cap B) \neq P(A) \cdot P(B)$.

Solution Because $A \cap B = \varnothing$, $P(A \cap B) = 0$ by probability axiom 2. But $P(A) \cdot P(B) \neq 0$ because neither $P(A)$ nor $P(B)$ equals zero. Thus $P(A \cap B) \neq P(A) \cdot P(B)$. ■

The following example and its immediate consequence show how the independence of two events extends to their complements.

Example 9.9.5 **The Probability of $A \cap B^c$ When A and B Are Independent Events**

Suppose A and B are independent events in a sample space S. Show that A and B^c are also independent.

Solution The solutions for exercises 8 and 28 in Section 6.2 show that for all sets A and B,

$$(1)\ (A \cap B) \cup (A \cap B^c) = A$$

and

$$(2)\ (A \cap B) \cap (A \cap B^c) = \varnothing.$$

It follows that probability axiom 3 may be applied to equation (1) to obtain

$$P((A \cap B) \cup (A \cap B^c)) = P(A \cap B) + P(A \cap B^c) = P(A).$$

Solving for $P(A \cap B^c)$ gives that

$$\begin{aligned} P(A \cap B^c) &= P(A) - P(A \cap B) \\ &= P(A) - P(A) \cdot P(B) && \text{because } A \text{ and } B \text{ are independent} \\ &= P(A)(1 - P(B)) && \text{by factoring out } P(A) \\ &= P(A) \cdot P(B^c) && \text{by formula 9.8.1.} \end{aligned}$$

Thus A and B^c are independent events. ■

It follows immediately from Example 9.9.5 that if A and B are independent, then A^c and B are also independent and so are A^c and B^c. (See exercise 22 at the end of this section.) These results are applied in Example 9.9.6.

Example 9.9.6 **Computing Probabilities of Intersections of Two Independent Events**

A coin is loaded so that the probability of heads is 0.6. Suppose the coin is tossed twice. Although the probability of heads is greater than the probability of tails, there is no reason to believe that whether the coin lands heads or tails on one toss will affect whether it lands heads or tails on the other toss. Thus it is reasonable to assume that the results of the tosses are independent.

a. What is the probability of obtaining two heads?

b. What is the probability of obtaining one head?

c. What is the probability of obtaining no heads?

d. What is the probability of obtaining at least one head?

Solution The sample space S consists of the four outcomes $\{HH, HT, TH, TT\}$, which are not equally likely. Let E be the event that a head is obtained on the first toss, and let F be the event that a head is obtained on the second toss. Then $P(E) = P(F) = 0.6$, and it is to be assumed that E and F are independent.

a. The event of obtaining two heads is $E \cap F$. And because E and F are independent,

$$P(\text{two heads}) = P(E \cap F) = P(E) \cdot P(F) = (0.6)(0.6) = 0.36 = 36\%.$$

b. One head can be obtained in two mutually exclusive ways: head on the first toss and tail on the second, or tail on the first toss and head on the second. Thus, the event of obtaining exactly one head is $(E \cap F^c) \cup (E^c \cap F)$. Also $(E \cap F^c) \cap (E^c \cap F) = \varnothing$, and, moreover, by the formula for the probability of the complement of an event, $P(E^c) = P(F^c) = 1 - 0.6 = 0.4$. Hence

$$\begin{aligned} P(\text{one head}) &= P((E \cap F^c) \cup (E^c \cap F)) \\ &= P(E)\cdot P(F^c) + P(E^c)\cdot P(F) && \text{by Example 9.9.5 and exercise 22} \\ &= (0.6)(0.4) + (0.4)(0.6) \\ &= 0.48 = 48\%. \end{aligned}$$

c. The event of obtaining no heads is $E^c \cap F^c$. Thus, by exercise 22,

$$P(\text{no heads}) = P(E^c \cap F^c) = P(E^c)\cdot P(F^c) = (0.4)(0.4) = 0.16 = 16\%.$$

d. There are two ways to solve this problem. One is to observe that because the event of obtaining one head and the event of obtaining two heads are mutually disjoint,

$$\begin{aligned} P(\text{at least one head}) &= P(\text{one head}) + P(\text{two heads}) \\ &= 0.48 + 0.36 && \text{by parts (a) and (b)} \\ &= 0.84 = 84\%. \end{aligned}$$

The second way is to use the fact that the event of obtaining at least one head is the complement of the event of obtaining no heads. So

$$\begin{aligned} P(\text{at least one head}) &= 1 - P(\text{no heads}) \\ &= 1 - 0.16 && \text{by part (c)} \\ &= 0.84 = 84\%. \end{aligned}$$

■

Example 9.9.7 **Expected Value of Tossing a Loaded Coin Twice**

Suppose that a coin is loaded so that the probability of heads is 0.6, and suppose the coin is tossed twice. If this experiment is repeated many times, what is the expected value of the number of heads?

Solution Think of the outcomes of the coin tosses as just 0, 1, or 2 heads. Example 9.9.6 showed that the probabilities of these outcomes are 0.16, 0.48, and 0.36, respectively. Thus, by definition of expected value, the

$$\text{expected number of heads} = 0\cdot(0.16) + 1\cdot(0.48) + 2\cdot(0.36) = 1.2.$$

■

What if a loaded coin is tossed more than twice? Suppose it is tossed ten times, or a hundred times. What are the probabilities of various numbers of heads?

The previous examples illustrated the fact that the probability of an intersection of two events is the product of their probabilities whenever the two events are independent. Is there a way to generalize the concept of independence so that the probability of the intersection of more than two events can be found by multiplying their probabilities?

To answer this question, we first define three events A, B, and C to be *pairwise independent* if, and only if,

$$P(A \cap B) = P(A)\cdot P(B),\ P(A \cap C) = P(A)\cdot P(C), \text{ and } P(B \cap C) = P(B)\cdot P(C).$$

However, as the next example shows, events can be pairwise independent without having the probability of their intersection be the product of their probabilities. Moreover, events can satisfy the condition $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$ without being pairwise independent (see exercise 26 at the end of this section).

Example 9.9.8 **Exploring Independence for Three Events**

Suppose that a fair coin is tossed twice. Let A be the event that a head is obtained on the first toss, B the event that a head is obtained on the second toss, and C the event that either two heads or two tails are obtained. Show that A, B, and C are pairwise independent but do not satisfy the condition $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$.

Solution Because there are four equally likely outcomes—HH, HT, TH, and TT—it is clear that $P(A) = P(B) = P(C) = \frac{1}{2}$. You can also see that $A \cap B = \{HH\}$, $A \cap C = \{HH\}$, $B \cap C = \{HH\}$, and $A \cap B \cap C = \{HH\}$. Hence $P(A \cap B) = P(A \cap C) = P(B \cap C) = \frac{1}{4}$, and so $P(A \cap B) = P(A)\cdot P(B)$, $P(A \cap C) = P(A)\cdot P(C)$, and $P(B \cap C) = P(B)\cdot P(C)$. Thus A, B, and C are pairwise independent. However,

$$P(A \cap B \cap C) = P(\{HH\}) = \frac{1}{4} \neq \left(\frac{1}{2}\right)^3 = P(A)\cdot P(B)\cdot P(C)$$ ■

Because of situations like the ones in Example 9.9.8 and exercise 26, four conditions must be included in the definition of independence for three events.

Definition

Let A, B, and C be events in a sample space S. A, B, and C are **pairwise independent** if, and only if, they satisfy conditions 1–3 below. They are **mutually independent** if, and only if, they satisfy all four conditions below.

1. $P(A \cap B) = P(A)\cdot P(B)$
2. $P(A \cap C) = P(A)\cdot P(C)$
3. $P(B \cap C) = P(B)\cdot P(C)$
4. $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$

The definition of mutual independence for any collection of n events with $n \geq 2$ generalizes the two definitions given previously.

Definition

Events $A_1, A_2, A_3, \ldots, A_n$ in a sample space S are **mutually independent** if, and only if, the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset.

Example 9.9.9 **Tossing a Loaded Coin Ten Times**

A coin is loaded so that the probability of heads is 0.6 (and thus the probability of tails is 0.4). Suppose the coin is tossed ten times. As in Example 9.9.6, it is reasonable to assume that the results of the tosses are mutually independent.

a. What is the probability of obtaining eight heads?

b. What is the probability of obtaining at least eight heads?

Solution

a. For each $i = 1, 2, \ldots, 10$, let H_i be the event that a head is obtained on the ith toss, and let T_i be the event that a tail is obtained on the ith toss. Suppose that the eight

heads occur on the first eight tosses and that the remaining two tosses are tails. This is the event $H_1 \cap H_2 \cap H_3 \cap H_4 \cap H_5 \cap H_6 \cap H_7 \cap H_8 \cap T_9 \cap T_{10}$. For simplicity, we denote it as *HHHHHHHHTT*. By definition of mutually independent events,

$$P(HHHHHHHHTT) = (0.6)^8(0.4)^2.$$

Because of the commutative law for multiplication, if the eight heads occur on any other of the ten tosses, the same number is obtained. For instance, if we denote the event $H_1 \cap H_2 \cap T_3 \cap H_4 \cap H_5 \cap H_6 \cap H_7 \cap H_8 \cap T_9 \cap H_{10}$ by *H H T H H H H H T H*, then

$$P(HHTHHHHHTH) = (0.6)^2(0.4)(0.6)^5(0.4)(0.6) = (0.6)^8(0.4)^2.$$

Now there are as many different ways to obtain eight heads in ten tosses as there are subsets of eight elements (the toss numbers on which heads are obtained) that can be chosen from a set of ten elements. This number is $\binom{10}{8}$. It follows that, because the different ways of obtaining eight heads are all mutually exclusive,

$$P(\text{eight heads}) = \binom{10}{8}(0.6)^8(0.4)^2.$$

b. By reasoning similar to that in part (a),

$$P(\text{nine heads}) = \begin{bmatrix}\text{the number of different}\\ \text{ways nine heads can be}\\ \text{obtained in ten tosses}\end{bmatrix} \cdot (0.6)^9(0.4)^1 = \binom{10}{9}(0.6)^9(0.4),$$

and

$$P(\text{ten heads}) = \begin{bmatrix}\text{the number of different}\\ \text{ways ten heads can be}\\ \text{obtained in ten tosses}\end{bmatrix} \cdot (0.6)^{10}(0.4)^0 = \binom{10}{10}(0.6)^{10}.$$

Because obtaining eight, obtaining nine, and obtaining ten heads are mutually disjoint events,

$$\begin{aligned} P(\text{at least eight heads}) &= P(\text{eight heads}) + P(\text{nine heads}) + P(\text{ten heads}) \\ &= \binom{10}{8}(0.6)^8(0.4)^2 + \binom{10}{9}(0.6)^9(0.4) + \binom{10}{10}(0.6)^{10} \\ &\cong 0.167 = 16.7\%. \end{aligned}$$

■

Note Binomial probabilities occur in situations with multiple, mutually independent repetitions of a random process, all of which have the same two possible outcomes with the same probabilities on each repetition.

Note the occurrence of the binomial coefficients $\binom{n}{k}$ in solutions to problems like the one in Example 9.9.9. For that reason, probabilities of the form

$$\binom{n}{k}p^{n-k}(1-p)^k,$$

where $0 \le p \le 1$, are called **binomial probabilities**.

TEST YOURSELF

1. If A and B are any events in a sample space S and $P(A) \neq 0$, then the conditional probability of B given A, denoted $P(B|A)$, equals _____.

2. Bayes' theorem says that if a sample space S is a union of mutually disjoint events $B_1, B_2, \ldots, B_n$, each with a nonzero probability, if A is an event

in S with $P(A) \neq 0$, and if k is an integer with $1 \leq k \leq n$, then _____.

3. Events A and B in a sample space S are independent if, and only if, _____.

4. Events A, B, and C in a sample space S are mutually independent if, and only if, _____, _____, _____, and _____.

EXERCISE SET 9.9

1. Suppose $P(A|B) = 1/2$ and $P(A \cap B) = 1/6$. What is $P(B)$?

2. Suppose $P(X|Y) = 1/3$ and $P(Y) = 1/4$. What is $P(X \cap Y)$?

H 3. The instructor of a discrete mathematics class gave two tests. Twenty-five percent of the students received an A on the first test and 15% of the students received A's on both tests. What percent of the students who received A's on the first test also received A's on the second test?

4. a. Prove that if A and B are any events in a sample space S, with $P(B) \neq 0$, then $P(A^c|B) = 1 - P(A|B)$.
   b. Explain how the result in part (a) justifies the following statements: (1) If the probability of a false positive on a test for a condition is 4%, then there is a 96% probability that a person who does not have the condition will have a negative test result. (2) If the probability of a false negative on a test for a condition is 1%, then there is a 99% probability that a person who does have the condition will test positive for it.

H 5. Suppose that A and B are events in a sample space S and that $P(A)$, $P(B)$, and $P(A|B)$ are known. Derive a formula for $P(A|B^c)$.

6. An urn contains 25 red balls and 15 blue balls. Two are chosen at random, one after the other, without replacement.
   a. Use a tree diagram to help calculate the following probabilities: the probability that both balls are red, the probability that the first ball is red and the second is not, the probability that the first ball is not red and the second is red, the probability that neither ball is red.
   b. What is the probability that the second ball is red?
   c. What is the probability that at least one of the balls is red?

7. Redo exercise 6 assuming that the urn contains 30 red balls and 40 blue balls.

8. A pool of 10 semifinalists for a job consists of 7 men and 3 women. Because all are considered equally qualified, the names of two of the semifinalists are drawn, one after the other, at random, to become finalists for the job.
   a. What is the probability that both finalists are women?
   b. What is the probability that both finalists are men?
   H c. What is the probability that one finalist is a woman and the other is a man?

H 9. Prove Bayes' theorem for $n = 2$. That is, prove that if a sample space S is a union of mutually disjoint events B_1 and B_2, if A is an event in S with $P(A) \neq 0$, and if $k = 1$ or $k = 2$, then

$$P(B_k|A) = \frac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2)}.$$

10. Prove the full version of Bayes' theorem.

11. One urn contains 12 blue balls and 7 white balls, and a second urn contains 8 blue balls and 19 white balls. An urn is selected at random, and a ball is chosen from the urn.
   a. What is the probability that the chosen ball is blue?
   b. If the chosen ball is blue, what is the probability that it came from the first urn?

12. Redo exercise 11 assuming that the first urn contains 4 blue balls and 16 white balls and the second urn contains 10 blue balls and 9 white balls.

H 13. One urn contains 10 red balls and 25 green balls, and a second urn contains 22 red balls and 15 green balls. A ball is chosen as follows: First an urn is selected by tossing a loaded coin with probability 0.4 of landing heads up and probability 0.6 of landing tails up. If the coin lands heads up, the first urn is chosen; otherwise, the second urn is chosen. Then a ball is picked at random from the chosen urn.
   a. What is the probability that the chosen ball is green?

b. If the chosen ball is green, what is the probability that it was picked from the first urn?

14. A drug-screening test is used in a large population of people of whom 4% actually use drugs. Suppose that the false positive rate is 3% and the false negative rate is 2%. Thus a person who uses drugs tests positive for them 98% of the time, and a person who does not use drugs tests negative for them 97% of the time.

a. What is the probability that a randomly chosen person who tests positive for drugs actually uses drugs?

b. What is the probability that a randomly chosen person who tests negative for drugs does not use drugs?

15. Two different factories both produce a certain automobile part. The probability that a component from the first factory is defective is 2%, and the probability that a component from the second factory is defective is 5%. In a supply of 180 of the parts, 100 were obtained from the first factory and 80 from the second factory.

a. What is the probability that a part chosen at random from the 180 is from the first factory?

b. What is the probability that a part chosen at random from the 180 is from the second factory?

c. What is the probability that a part chosen at random from the 180 is defective?

d. If the chosen part is defective, what is the probability that it came from the first factory?

***H* 16.** Three different suppliers—X, Y, and Z—provide produce for a grocery store. Twelve percent of produce from X is superior grade, 8% of produce from Y is superior grade, and 15% of produce from Z is superior grade. The store obtains 20% of its produce from X, 45% from Y, and 35% from Z.

a. If a piece of produce is purchased, what is the probability that it is superior grade?

b. If a piece of produce in the store is superior grade, what is the probability that it is from X?

17. Prove that if A and B are events in a sample space S with the property that $P(A|B) = P(A)$ and $P(A) \neq 0$, then $P(B|A) = P(B)$.

18. Prove that if $P(A \cap B) = P(A) \cdot P(B)$, $P(A) \neq 0$, and $P(B) \neq 0$, then $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

19. A pair of fair dice, one blue and the other gray, are rolled. Let A be the event that the number face up on the blue die is 2, and let B be the event that the number face up on the gray die is 4 or 5. Show that $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

20. Suppose a fair coin is tossed three times. Let A be the event that a head appears on the first toss, and let B be the event that an even number of heads is obtained. Show that $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

21. If A and B are events in a sample space S and $A \cap B = \varnothing$, what must be true in order for A and B to be independent? Explain.

22. Prove that if A and B are independent events in a sample space S, then A^c and B are also independent, and so are A^c and B^c.

23. A student taking a multiple-choice exam does not know the answers to two questions. All have five choices for the answer. For one of the two questions, the student can eliminate two answer choices as incorrect but has no idea about the other answer choices. For the other question, the student has no clue about the correct answer at all. Assume that whether the student chooses the correct answer on one of the questions does not affect whether the student chooses the correct answer on the other question.

a. What is the probability that the student will answer both questions correctly?

b. What is the probability that the student will answer exactly one of the questions correctly?

c. What is the probability that the student will answer neither question correctly?

24. A software company uses two quality assurance (QA) checkers X and Y to check an application for bugs. X misses 12% of the bugs and Y misses 15%. Assume that the QA checkers work independently.

a. What is the probability that a randomly chosen bug will be missed by both QA checkers?

b. If the program contains 1,000 bugs, what number can be expected to be missed?

25. A coin is loaded so that the probability of heads is 0.7 and the probability of tails is 0.3. Suppose that the coin is tossed twice and that the results of the tosses are independent.

a. What is the probability of obtaining exactly two heads?

b. What is the probability of obtaining exactly one head?

c. What is the probability of obtaining no heads?

d. What is the probability of obtaining at least one head?

* **26.** Describe a sample space and events A, B, and C, where $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$ but A, B, and C are not pairwise independent.

H **27.** The example used to introduce conditional probability described a family with two children each of whom was equally likely to be a boy or a girl. The example showed that if it is known that one child is a boy, the probability that the other child is a boy is $1/3$. Now imagine the same kind of family—two children each of whom is equally likely to be a boy or a girl. Suppose you meet one of the children and that child is a boy. What is the probability that the other child is a boy? Explain. (Be careful. The answer may surprise you.)

28. A coin is loaded so that the probability of heads is 0.7 and the probability of tails is 0.3. Suppose that the coin is tossed ten times and that the results of the tosses are mutually independent.

a. What is the probability of obtaining exactly seven heads?

b. What is the probability of obtaining exactly ten heads?

c. What is the probability of obtaining no heads?

d. What is the probability of obtaining at least one head?

29. Suppose that ten items are chosen at random from a large batch delivered to a company. The manufacturer claims that just 3% of the items in the batch are defective. Assume that the batch is large enough so that even though the selection is made without replacement, the number 0.03 can be used to approximate the probability that any one of the ten items is defective. In addition, assume that because the items are chosen at random, the outcomes of the choices are mutually independent. Finally, assume that the manufacturer's claim is correct.

a. What is the probability that none of the ten is defective?

b. What is the probability that at least one of the ten is defective?

c. What is the probability that exactly four of the ten are defective?

d. What is the probability that at most two of the ten are defective?

30. Suppose the probability of a false positive result on a mammogram is 4% and that radiologists' interpretations of mammograms are mutually independent in the sense that whether or not a radiologist finds a positive result on one mammogram does not influence whether or not a radiologist finds a positive result on another mammogram. Assume that a woman has a mammogram every year for ten years.

a. What is the probability that she will have no false positive results during that time?

b. What is the probability that she will have at least one false positive result during that time?

c. What is the probability that she will have exactly two false positive results during that time?

d. Suppose that the probability of a false negative result on a mammogram is 2%, and assume that the probability that a randomly chosen woman has breast cancer is 0.0002.

(i) If a woman has a positive test result one year, what is the probability that she actually has breast cancer?

(ii) If a woman has a negative test result one year, what is the probability that she actually has breast cancer?

31. Empirical data indicate that approximately 103 out of every 200 children born are male. Hence the probability of a newborn being male is about 51.5%. Suppose that a family has six children, and suppose that the genders of all the children are mutually independent.

H **a.** What is the probability that none of the children is male?

b. What is the probability that at least one of the children is male?

c. What is the probability that exactly five of the children are male?

32. A person takes a multiple-choice exam in which each question has four possible answers. Suppose that the person has no idea about the answers to three of the questions and simply chooses randomly for each one.

a. What is the probability that the person will answer all three questions correctly?

b. What is the probability that the person will answer exactly two questions correctly?

c. What is the probability that the person will answer exactly one question correctly?

d. What is the probability that the person will answer no questions correctly?

e. Suppose that the person gets one point of credit for each correct answer and that $1/3$ point

is deducted for each incorrect answer. What is the expected value of the person's score for the three questions?

33. In exercise 23 of Section 9.8, let C_k be the event that the gambler has k dollars, wins the next roll of the die, and is eventually ruined, let D_k be the event that the gambler has k dollars, loses the next roll of the die, and is eventually ruined, and let P_k be the probability that the gambler is eventually ruined if he has k dollars. Use the probability axioms and the definition of conditional probability to derive the equation

$$P_{k-1} = \frac{1}{6}P_k + \frac{5}{6}P_{k-2}.$$

***H* 34.** Use conditional probability to analyze exercise 20 in Section 9.1. Let X be the event that the prize is not behind door A, and let Y be the event that you switch and choose the door with the prize. Should you switch? Explain why or why not.

ANSWERS FOR TEST YOURSELF

1. $\dfrac{P(A \cap B)}{P(A)}$ **2.** $P(B_k|A) = \dfrac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots + P(A|B_n)P(B_n)}$ **3.** $P(A \cap B) = P(A) \cdot P(B)$

4. $P(A \cap B) = P(A) \cdot P(B)$; $P(A \cap C) = P(A) \cdot P(C)$; $P(B \cap C) = P(B) \cdot P(C)$; $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

CHAPTER 10 THEORY OF GRAPHS AND TREES

Throughout the book graphs and trees have been used as convenient visualizations. For instance, a graph can model a wide variety of structures such as the arrangement of electric power lines or fiber optic cables, a transportation system, a knowledge base, or a collection of computers ranging from a small local area network to the entire world wide web. A graph model can be used to solve a logical problem, color a map, or schedule meetings. A possibility tree shows all potential results of a multistep operation with a finite number of outcomes for each step, the directed graph of a relation on a set shows which element of the set are related to which, a Hasse diagram illustrates the relations among elements in a partially ordered set, and a PERT diagram shows which tasks must precede which in executing a project.

In Chapter 1 we introduced the basic terminology of graphs, and in Section 4.9 we used properties of even and odd integers and direct and indirect proof to prove the handshake theorem and derive some of its consequences. We first proved the formula for the number of edges in a complete graph on n vertices using the handshake theorem, and then reproved it using mathematical induction in Section 5.3, recursion in Section 5.6, and combinatorial reasoning in Section 9.5.

In this chapter we go more deeply into the mathematics of graphs and trees by exploring the concepts of connectedness, Euler and Hamiltonian circuits, representation of graphs by matrices, isomorphisms of graphs, the relations between the number of vertices and the number of edges in a tree, properties of rooted trees, spanning trees, and finding shortest paths in graphs. Applications include uses of graphs and trees in the study of decision problems, chemistry, data storage, computer language syntax, and transportation networks.

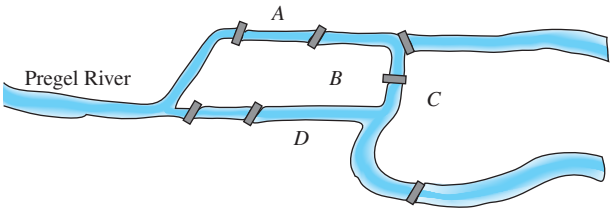
10.1 Trails, Paths, and Circuits

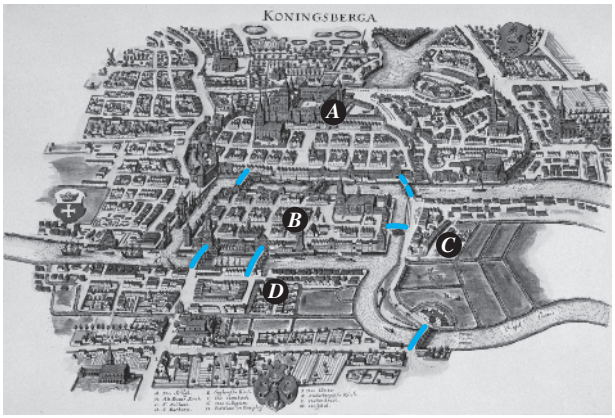
One can begin to reason only when a clear picture has been formed in the imagination. —W. W. Sawyer, *Mathematician's Delight*, 1943

The subject of graph theory began in the year 1736 when the great mathematician Leonhard Euler published a paper giving the solution to the following puzzle:

> The town of Königsberg in Prussia (now Kaliningrad in Russia) was built at a point where two branches of the Pregel River came together. It consisted of an island and some land along the river banks. These were connected by seven bridges as shown in Figure 10.1.1.
>
> The question is this: Is it possible for a person to take a walk around town, starting and ending at the same location and crossing each of the seven bridges exactly once?*

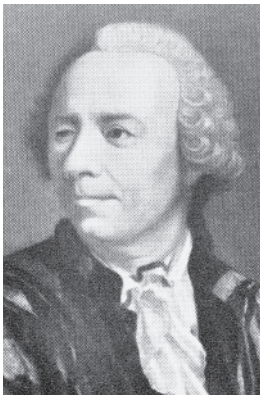
*In his original paper, Euler did not require the walk to start and end at the same point. The analysis of the problem is simplified, however, by adding this condition. Later in the section we discuss walks that start and end at different points.





AKG Images

FIGURE 10.1.1 The Seven Bridges of Königsberg



Bettmann/Getty Images

Leonhard Euler
(1707–1783)

To solve this puzzle, Euler translated it into a graph theory problem. He noticed that all points of a given land mass can be identified with each other since a person can travel from any one point to any other point of the same land mass without crossing a bridge. Thus for the purpose of solving the puzzle, the map of Königsberg can be identified with the graph shown in Figure 10.1.2, in which the vertices A, B, C, and D represent land masses and the seven edges represent the seven bridges.

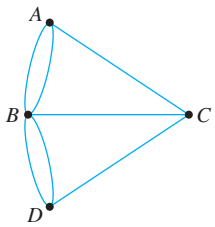


FIGURE 10.1.2 Graph Version of Königsberg Map

In terms of this graph, the question becomes the following:

> Is it possible to find a route through the graph that starts and ends at some vertex, one of A, B, C, or D, and traverses each edge exactly once?

Equivalently:

> Is it possible to trace this entire graph, starting and ending at the same point, without either ever lifting your pencil from the paper or crossing an edge more than once?

Take a few minutes to think about the question yourself. Can you find a route that meets the requirements? Try it!

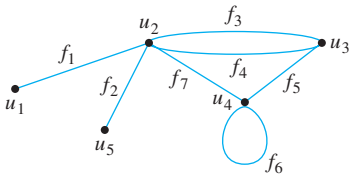
Looking for a route is frustrating because you continually find yourself at a vertex that does not have an unused edge on which to leave, while elsewhere there are unused edges that must still be traversed. If you start at vertex A, for example, each time you pass through vertex B, C, or D, you use up two edges because you arrive on one edge and depart on a different one. So, if it is possible to find a route that uses all the edges

of the graph and starts and ends at A, then the total number of arrivals and departures from each vertex B, C, and D must be a multiple of 2. Or, in other words, the degrees of the vertices B, C, and D must be even. But they are not: $\deg(B) = 5$, $\deg(C) = 3$, and $\deg(D) = 3$. Hence there is no route that solves the puzzle by starting and ending at A. Similar reasoning can be used to show that there are no routes that solve the puzzle by starting and ending at B, C, or D. Therefore, it is impossible to travel all around the city crossing each bridge exactly once.

Definitions

Travel in a graph is accomplished by moving from one vertex to another along a sequence of adjacent edges. In the graph below, for instance, you can go from u_1 to u_4 by taking f_1 to u_2 and then f_7 to u_4. This is represented by writing

$$u_1 f_1 u_2 f_7 u_4.$$



Or you could take the roundabout route

$$u_1 f_1 u_2 f_3 u_3 f_4 u_2 f_3 u_3 f_5 u_4 f_6 u_4 f_7 u_2 f_3 u_3 f_5 u_4.$$

Certain types of sequences of adjacent vertices and edges are of special importance in graph theory: those that do not have a repeated edge, those that do not have a repeated vertex, and those that start and end at the same vertex.

Definition

Let G be a graph, and let v and w be vertices in G.

A **walk from v to w** is a finite alternating sequence of adjacent vertices and edges of G. Thus a walk has the form

$$v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n,$$

where the v's represent vertices, the e's represent edges, $v_0 = v$, $v_n = w$, and for each $i = 1, 2, \ldots n$, v_{i-1} and v_i are the endpoints of e_i. The **trivial walk from v to v** consists of the single vertex v.

A **trail from v to w** is a walk from v to w that does not contain a repeated edge.

A **path from v to w** is a trail that does not contain a repeated vertex.

A **closed walk** is a walk that starts and ends at the same vertex.

A **circuit** is a closed walk that contains at least one edge and does not contain a repeated edge.

A **simple circuit** is a circuit that does not have any other repeated vertex except the first and last.

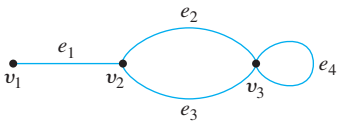
For ease of reference, these definitions are summarized in the following table:

	Repeated Edge?	Repeated Vertex?	Starts and Ends at the Same Point?	Must Contain at Least One Edge?
Walk	allowed	allowed	allowed	no
Trail	no	allowed	allowed	no
Path	no	no	no	no
Closed walk	allowed	allowed	yes	no
Circuit	no	allowed	yes	yes
Simple circuit	no	first and last only	yes	yes

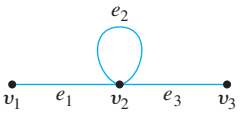
Often a walk can be specified unambiguously by giving either a sequence of edges or a sequence of vertices. The next two examples show how this is done.

Example 10.1.1 **Notation for Walks**

a. In the graph below, the notation $e_1e_2e_4e_3$ refers unambiguously to the following walk: $v_1e_1v_2e_2v_3e_4v_3e_3v_2$. On the other hand, the notation e_1 is ambiguous if used by itself to refer to a walk. It could mean either $v_1e_1v_2$ or $v_2e_1v_1$.



b. In the graph of part (a), the notation v_2v_3 is ambiguous if used to refer to a walk. It could mean $v_2e_2v_3$ or $v_2e_3v_3$. On the other hand, in the graph below, the notation $v_1v_2v_2v_3$ refers unambiguously to the walk $v_1e_1v_2e_2v_2e_3v_3$.



■

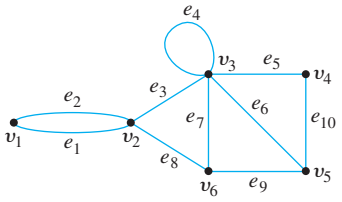
Note that if a graph G does not have any parallel edges, then any walk in G is uniquely determined by its sequence of vertices.

Example 10.1.2 **Walks, Trails, Paths, and Circuits**

In the graph below, determine which of the following walks are trails, paths, circuits, or simple circuits.

a. $v_1e_1v_2e_3v_3e_4v_3e_5v_4$ b. $e_1e_3e_5e_5e_6$ c. $v_2v_3v_4v_5v_3v_6v_2$

d. $v_2v_3v_4v_5v_6v_2$ e. $v_1e_1v_2e_1v_1$ f. v_1



Solution

a. This walk has a repeated vertex but does not have a repeated edge, so it is a trail from v_1 to v_4 but not a path.

b. This is just a walk from v_1 to v_5. It is not a trail because it has a repeated edge.

c. This walk starts and ends at v_2, contains at least one edge, and does not have a repeated edge, so it is a circuit. Since the vertex v_3 is repeated in the middle, it is not a simple circuit.

d. This walk starts and ends at v_2, contains at least one edge, does not have a repeated edge, and does not have a repeated vertex. Thus it is a simple circuit.

e. This is just a closed walk starting and ending at v_1. It is not a circuit because edge e_1 is repeated.

f. The first vertex of this walk is the same as its last vertex, but it does not contain an edge, and so it is not a circuit. It is a closed walk from v_1 to v_1. (It is also a trail from v_1 to v_1.) ■

Because most of the major developments in graph theory have happened relatively recently and in a variety of different contexts, the terms used in the subject have not been standardized. For example, what this book calls a *graph* is sometimes called a *multigraph*, what this book calls a *simple graph* is sometimes called a *graph*, what this book calls a *vertex* is sometimes called a *node*, and what this book calls an *edge* is sometimes called an *arc*. Similarly, instead of the word *trail*, the word *path* is sometimes used; instead of the word *path*, the words *simple path* are sometimes used; and instead of the words *simple circuit*, the word *cycle* is sometimes used. The terminology in this book is among the most common, but if you consult other sources, be sure to check their definitions.

Subgraphs

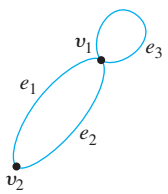
Definition

A graph H is said to be a **subgraph** of a graph G if, and only if, every vertex in H is also a vertex in G, every edge in H is also an edge in G, and every edge in H has the same endpoints as it has in G.

Example 10.1.3 **Subgraphs**

List all subgraphs of the graph G with vertex set $\{v_1, v_2\}$ and edge set $\{e_1, e_2, e_3\}$, where the endpoints of e_1 are v_1 and v_2, the endpoints of e_2 are v_1 and v_2, and e_3 is a loop at v_1.

Solution G can be drawn as shown below.



There are 11 subgraphs of G, which can be grouped according to those that do not have any edges, those that have one edge, those that have two edges, and those that have three edges. The 11 subgraphs are shown in Figure 10.1.3 on the next page.

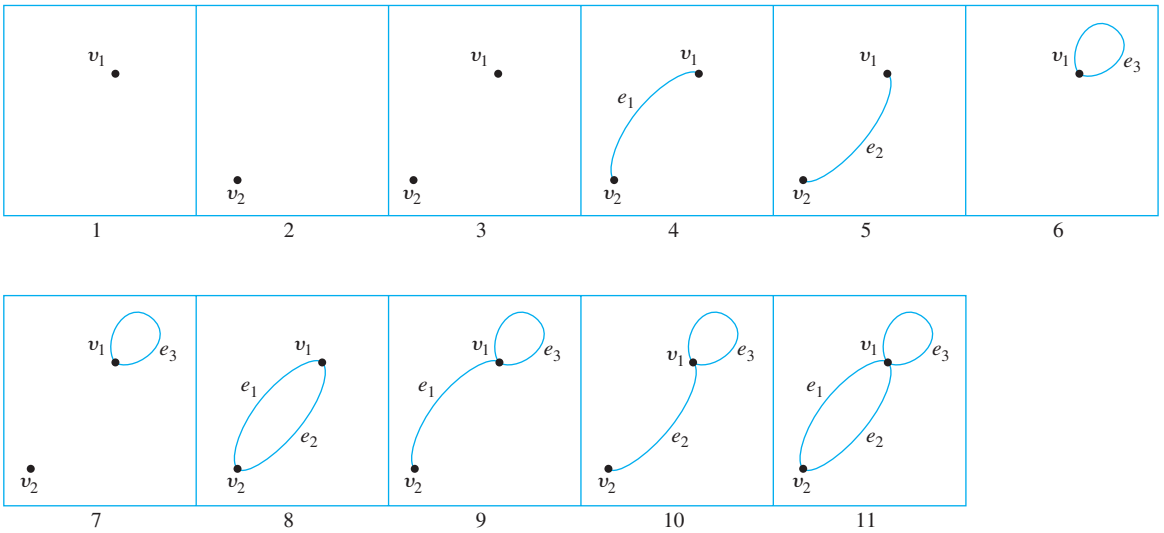


FIGURE 10.1.3

Connectedness

It is easy to understand the concept of connectedness on an intuitive level. Roughly speaking, a graph is connected if it is possible to travel from any vertex to any other vertex along a sequence of adjacent edges of the graph. The formal definition of connectedness is stated in terms of walks.

Definition

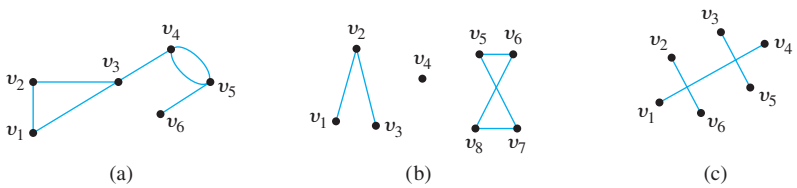
Let G be a graph. Two **vertices v and w of G are connected** if, and only if, there is a walk from v to w. The **graph G is connected** if, and only if, given *any* two vertices v and w in G, there is a walk from v to w. Symbolically:

$$G \text{ is connected} \iff \forall \text{ vertices } v \text{ and } w \text{ in } G, \exists \text{ a walk from } v \text{ to } w.$$

If you take the negation of this definition, you will see that a graph G is *not connected* if, and only if, there exist two vertices of G that are not connected by any walk.

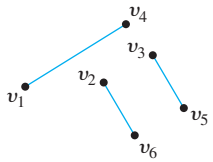
Example 10.1.4 **Connected and Disconnected Graphs**

Which of the following graphs are connected?



Solution The graph represented in (a) is connected, whereas those of (b) and (c) are not. To understand why (c) is not connected, recall that in a drawing of a graph, two

edges may cross at a point that is not a vertex. Thus the graph in (c) can be redrawn as follows:



■

Some useful facts relating circuits and connectedness are collected in the following lemma. Proofs of (a) and (b) are left for the exercises. The proof of (c) is in Section 10.4.

Lemma 10.1.1

Let G be a graph.

a. If G is connected, then any two distinct vertices of G can be connected by a path.

b. If vertices v and w are part of a circuit in G and one edge is removed from the circuit, then there still exists a trail from v to w in G.

c. If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.

Look back at Example 10.1.4. The graphs in (b) and (c) are both made up of three pieces, each of which is itself a connected graph. A *connected component* of a graph is a connected subgraph of largest possible size.

Definition

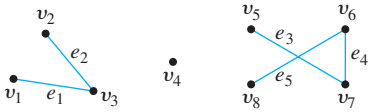
A graph H is a **connected component** of a graph G if, and only if,

1. H is subgraph of G;
2. H is connected; and
3. no connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H.

The fact is that any graph is a kind of union of its connected components.

Example 10.1.5 **Connected Components**

Find all connected components of the following graph G.



Solution G has three connected components: H_1, H_2, and H_3 with vertex sets V_1, V_2, and V_3 and edge sets E_1, E_2, and E_3, where

$$V_1 = \{v_1, v_2, v_3\}, \qquad E_1 = \{e_1, e_2\},$$
$$V_2 = \{v_4\}, \qquad E_2 = \varnothing,$$
$$V_3 = \{v_5, v_6, v_7, v_8\}, \qquad E_3 = \{e_3, e_4, e_5\}.$$

■

Euler Circuits

Now we return to consider general problems similar to the puzzle of the Königsberg bridges. The following definition is made in honor of Euler.

Definition

Let G be a graph. An **Euler circuit** for G is a circuit that contains every vertex and every edge of G. That is, an Euler circuit for G is a sequence of adjacent vertices and edges in G that has at least one edge, starts and ends at the same vertex, uses every vertex of G at least once, and uses every edge of G exactly once.

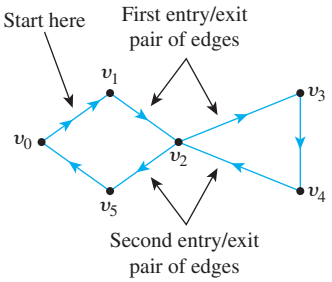
The analysis used earlier to solve the puzzle of the Königsberg bridges generalizes to prove the following theorem:

Theorem 10.1.2

If a graph has an Euler circuit, then every vertex of the graph has positive even degree.

Proof:

Suppose G is a graph that has an Euler circuit. *[We must show that given any vertex v of G, the degree of v is even.]* Let v be any particular but arbitrarily chosen vertex of G. Since the Euler circuit contains every edge of G, it contains all edges incident on v. Now imagine taking a journey that begins in the middle of one of the edges adjacent to the start of the Euler circuit and continues around the Euler circuit to end in the middle of the starting edge. (See Figure 10.1.4. There is such a starting edge because the Euler circuit has at least one edge.) Each time v is entered by traveling along one edge, it is immediately exited by traveling along another edge (since the journey ends in the *middle* of an edge).



In this example, the Euler circuit is $v_0v_1v_2v_3v_4v_2v_5v_0$, and v is v_2. Each time v_2 is entered by one edge, it is exited by another edge.

FIGURE 10.1.4 Example for the Proof of Theorem 10.1.2

Because the Euler circuit uses every edge of G exactly once, every edge incident on v is traversed exactly once in this process. Hence the edges incident on v occur in entry/exit pairs, and consequently the degree of v must be a positive multiple of 2. But that means that v has positive even degree *[as was to be shown]*.

Recall that the contrapositive of a statement is logically equivalent to the statement. The contrapositive of Theorem 10.1.2 is as follows:

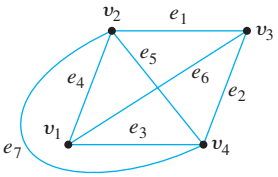
Contrapositive Version of Theorem 10.1.2

If some vertex of a graph has odd degree, then the graph does not have an Euler circuit.

This version of Theorem 10.1.2 is useful for showing that a given graph does *not* have an Euler circuit.

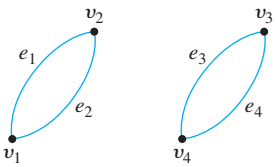
Example 10.1.6 **Showing That a Graph Does Not Have an Euler Circuit**

Show that the graph below does not have an Euler circuit.



Solution Vertices v_1 and v_3 both have degree 3, which is odd. Hence by (the contrapositive form of) Theorem 10.1.2, this graph does not have an Euler circuit. ■

Now consider the converse of Theorem 10.1.2: If every vertex of a graph has even degree, then the graph has an Euler circuit. Is this true? The answer is no. There is a graph G such that every vertex of G has even degree but G does not have an Euler circuit. In fact, there are many such graphs. The illustration below shows one example.



Every vertex has even degree, but the graph does not have an Euler circuit.

Note that the graph in the preceding drawing is not connected. It turns out that although the converse of Theorem 10.1.2 is false, a modified converse is true: If every vertex of a graph has positive even degree *and* if the graph is connected, then the graph has an Euler circuit. The proof of this fact is constructive: It contains an algorithm to find an Euler circuit for any connected graph in which every vertex has even degree.

Theorem 10.1.3

If a graph G is connected and the degree of every vertex of G is a positive even integer, then G has an Euler circuit.

Proof:

Suppose that G is any connected graph and suppose that every vertex of G is a positive even integer. *[We must find an Euler circuit for G.]* Construct a circuit C by the following algorithm:

Step 1: Pick any vertex v of G at which to start.
[This step can be accomplished because the vertex set of G is nonempty by assumption.]

Step 2: Pick any sequence of adjacent vertices and edges, starting and ending at v and never repeating an edge. Call the resulting circuit C.

(continued on page 686)

[This step can be performed for the following reasons: Since the degree of each vertex of G is a positive even integer, as each vertex of G is entered by traveling on one edge, either the vertex is v itself and there is no other unused edge adjacent to v, or the vertex can be exited by traveling on another previously unused edge. Since the number of edges of the graph is finite (by definition of graph), the sequence of distinct edges cannot go on forever. The sequence eventually returns to v because the degree of v is a positive even integer, and so each time an edge leads out from v to another vertex, there must be a different edge that connects back in to v.]

Step 3: Check whether C contains every edge and vertex of G. If so, C is an Euler circuit, and we are finished. If not, perform the following steps.

Step 3a: Remove all edges of C from G and also any vertices that become isolated when the edges of C are removed. Call the resulting subgraph G'.

[Note that G' may not be connected (as illustrated in Figure 10.1.5), but every vertex of G' has positive, even degree (since removing the edges of C removes an even number of edges from each vertex, the difference of two even integers is even, and isolated vertices with degree 0 were removed).]

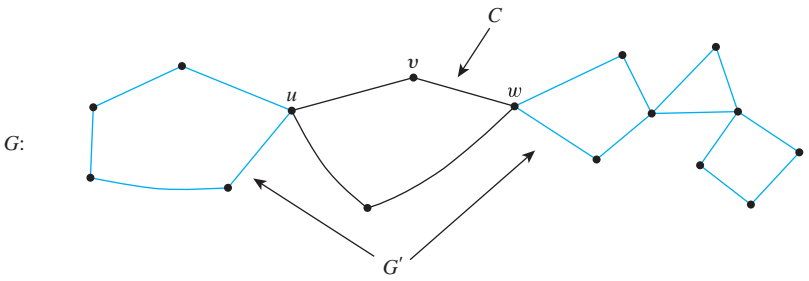


FIGURE 10.1.5

Step 3b: Pick any vertex w common to both C and G'.

[There must be at least one such vertex since G is connected. (See exercise 50.) (In Figure 10.1.5 there are two such vertices: u and w.)]

Step 3c: Pick any sequence of adjacent vertices and edges of G', starting and ending at w and never repeating an edge. Call the resulting circuit C'.

[This can be done since each vertex of G' has positive, even degree and G' is finite. See the justification for step 2.]

Step 3d: Patch C and C' together to create a new circuit C'' as follows: Start at v and follow C all the way to w. Then follow C' all the way back to w. After that, continue along the untraveled portion of C to return to v.

[The effect of executing steps 3c and 3d for the graph of Figure 10.1.5 is shown in Figure 10.1.6.]

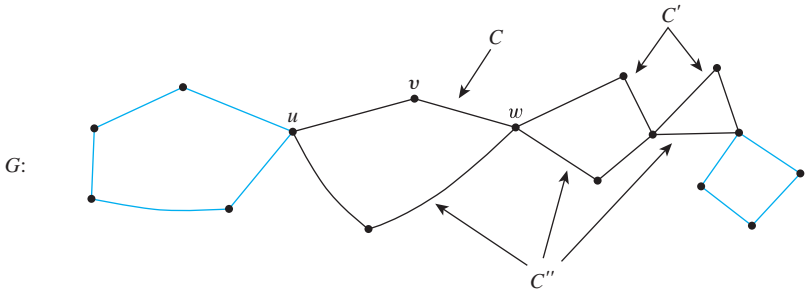


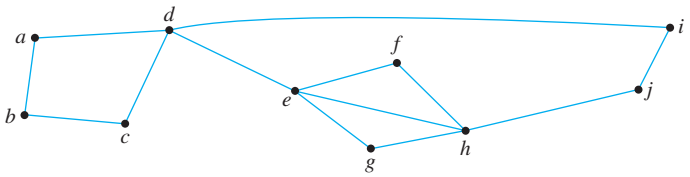
FIGURE 10.1.6

Step 3e: Let $C = C''$ and go back to step 3.

Since the graph G is finite, execution of the steps outlined in this algorithm must eventually terminate. At that point an Euler circuit for G will have been constructed. (Note that because of the element of choice in steps 1, 2, 3b, and 3c, a variety of different Euler circuits can be produced by using this algorithm.)

Example 10.1.7 **Finding an Euler Circuit**

Use Theorem 10.1.3 to check that the graph below has an Euler circuit. Then use the algorithm from the proof of the theorem to find an Euler circuit for the graph.



Solution Observe that

$$\deg(a) = \deg(b) = \deg(c) = \deg(f) = \deg(g) = \deg(i) = \deg(j) = 2$$

and that

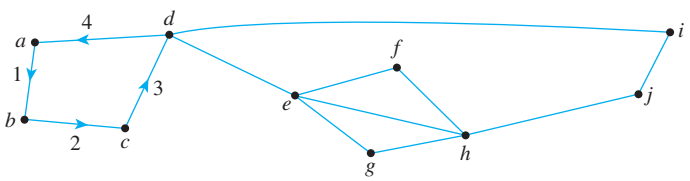
$$\deg(d) = \deg(e) = \deg(h) = 4.$$

Hence all vertices have even degree. Also, the graph is connected. Thus, by Theorem 10.1.3, the graph has an Euler circuit.

To construct an Euler circuit using the algorithm of Theorem 10.1.3, let $v = a$ and let C be

$$C\text{: } abcda.$$

C is represented by the labeled edges shown below.



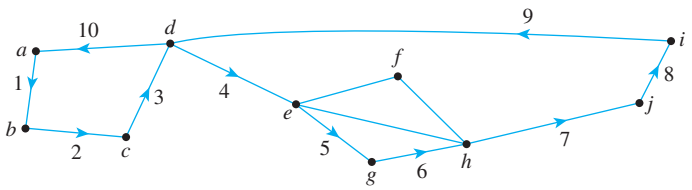
Observe that C is not an Euler circuit for the graph but that C intersects the rest of the graph at d. Let C' be

$$C'\text{: } deghjid.$$

Patch C' into C to obtain

$$C''\text{: } abcdeghjida.$$

Set $C = C''$. Then C is represented by the labeled edges shown below.



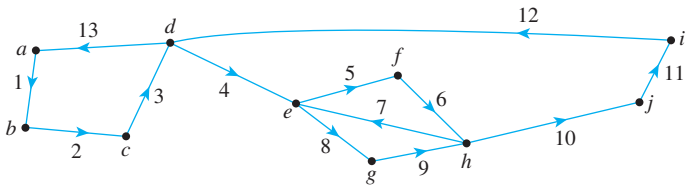
Observe that C is not an Euler circuit for the graph but that it intersects the rest of the graph at e and h. Let C' be

$$C'\text{: } efhe.$$

Patch C' into C to obtain

$$C''\text{: } abcdefheghjida.$$

Set $C = C''$. Then C is represented by the labeled edges shown below.



Since C includes every edge of the graph exactly once, C is an Euler circuit for the graph. ■

In exercise 51 at the end of this section you are asked to show that any graph with an Euler circuit is connected. This result can be combined with Theorems 10.1.2 and 10.1.3 to give a complete characterization of graphs that have Euler circuits, as stated in Theorem 10.1.4.

Theorem 10.1.4

A graph G has an Euler circuit if, and only if, G is connected and every vertex of G has positive even degree.

A corollary to Theorem 10.1.4 gives a criterion for determining when it is possible to find a walk from one vertex of a graph to another, passing through every vertex of the graph at least once and every edge of the graph exactly once.

Definition

Let G be a graph, and let v and w be two distinct vertices of G. An **Euler trail from v to w** is a sequence of adjacent edges and vertices that starts at v, ends at w, passes through every vertex of G at least once, and traverses every edge of G exactly once.

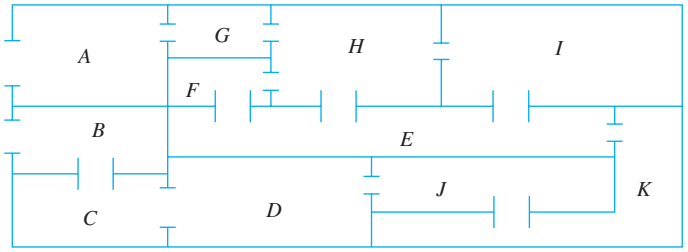
Corollary 10.1.5

Let G be a graph, and let v and w be two distinct vertices of G. There is an Euler trail from v to w if, and only if, G is connected, v and w have odd degree, and all other vertices of G have positive even degree.

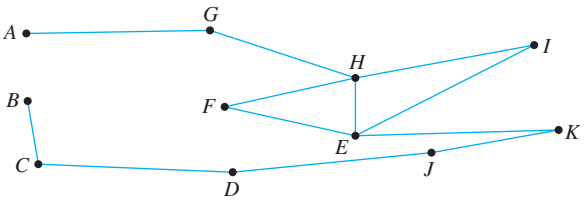
The proof of this corollary is left as an exercise.

Example 10.1.8 **Finding an Euler Trail**

The floor plan shown below is for a house that is open for public viewing. Is it possible to find a trail that starts in room A, ends in room B, and passes through every interior doorway of the house exactly once? If so, find such a trail.



Solution Let the floor plan of the house be represented by the graph below, where the edges indicate the openings between the rooms.



Each vertex of this graph has even degree except for A and B, each of which has degree 1. Hence by Corollary 10.1.5, there is an Euler trail from A to B. One such trail is

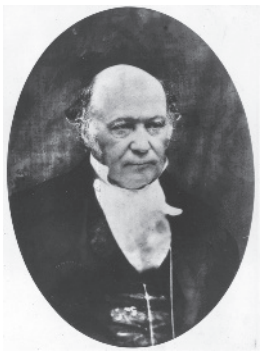
$$A\ G\ H\ F\ E\ I\ H\ E\ K\ J\ D\ C\ B.$$

■

Hamiltonian Circuits

Theorem 10.1.4 completely answers the following question: Given a graph G, is it possible to find a circuit for G in which all the *edges* of G appear exactly once? A related question is this: Given a graph G, is it possible to find a circuit for G in which all the *vertices* of G (except the first and the last) appear exactly once?

In 1859 the Irish mathematician Sir William Rowan Hamilton introduced a puzzle in the shape of a dodecahedron (DOH-dek-a-HEE-dron). (Figure 10.1.7 contains a drawing of a dodecahedron, which is a solid figure with 12 identical pentagonal faces.)



Hulton Archive/Getty Images

Sir William Hamilton (1805–1865)

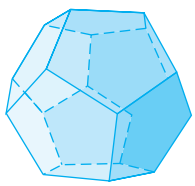
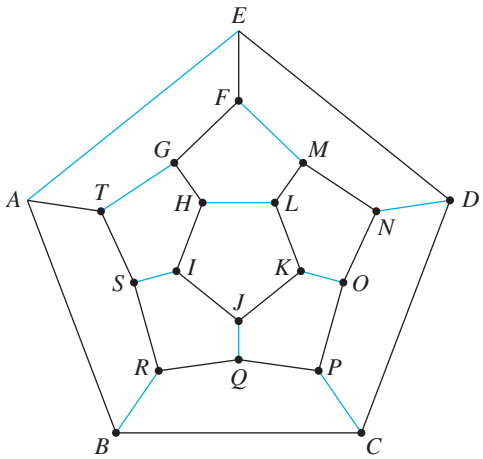


FIGURE 10.1.7 Dodecahedron

Each vertex was labeled with the name of a city—London, Paris, Hong Kong, New York, and so on. The problem Hamilton posed was to start at one city and tour the world by visiting each other city exactly once and returning to the starting city. One way to solve the puzzle is to imagine the surface of the dodecahedron stretched out and laid flat in the plane, as follows:



One solution is the circuit

$$A\,B\,C\,D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,A,$$

whose edges are indicated with black lines. Note that although every city is visited, many edges are omitted from the circuit. (More difficult versions of the puzzle required that certain cities be visited in a certain order.)

The following definition is made in honor of Hamilton.

Definition

Given a graph G, a **Hamiltonian circuit** for G is a simple circuit that includes every vertex of G. That is, a Hamiltonian circuit for G is a sequence of adjacent vertices and distinct edges in which every vertex of G appears exactly once, except for the first and the last, which are the same.

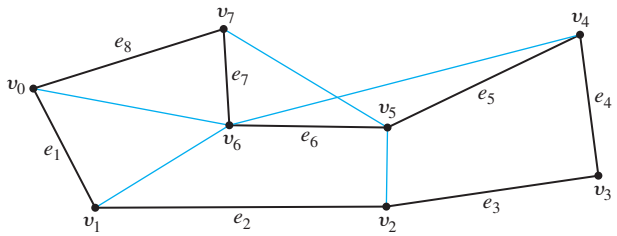
Note that although an Euler circuit for a graph G must include every vertex of G, it may visit some vertices more than once and hence may not be a Hamiltonian circuit. On the other hand, a Hamiltonian circuit for G does not need to include all the edges of G and hence may not be an Euler circuit.

Despite the analogous-sounding definitions of Euler and Hamiltonian circuits, the mathematics of the two are very different. Theorem 10.1.4 gives a simple criterion for determining whether a given graph has an Euler circuit. Unfortunately, there is no analogous criterion for determining whether a given graph has a Hamiltonian circuit, nor is there even an efficient algorithm for finding such a circuit. There is, however, a simple technique that can be used in many cases to show that a graph does *not* have a Hamiltonian circuit. This follows from the following considerations:

Suppose a graph G with at least two vertices has a Hamiltonian circuit C, given concretely as

$$C\colon v_0e_1v_1e_2\cdots v_{n-1}e_nv_n\,(=v_0).$$

Since C is a simple circuit, all the e_i are distinct and all the v_j are distinct except that $v_0 = v_n$. Let H be the subgraph of G that is formed using the vertices and edges of C. An example of such an H is shown below.



C: $v_0\, e_1 v_1 e_2\, v_2\, e_3 v_3\, e_4 v_4\, e_5 v_5\, e_6 v_6\, e_7 v_7 e_8\, v_0$

The edges of H are shown in black.

Note that H has the same number of edges as it has vertices since all its edges are distinct and so are its vertices. Also, by definition of Hamiltonian circuit, every vertex of G is a vertex of H, and H is connected since any two of its vertices lie on a circuit. In addition, every vertex of H has degree 2. The reason for this is that there are exactly two edges incident on any vertex. These are e_i and e_{i+1} for any vertex v_j except $v_0 = v_n$, and they are e_1 and e_n for $v_0 (= v_n)$. These observations have established the truth of the following proposition in all cases where G has at least two vertices.

Proposition 10.1.6

If a graph G has a Hamiltonian circuit, then G has a subgraph H with the following properties:

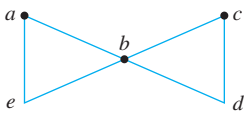
1. H contains every vertex of G.
2. H is connected.
3. H has the same number of edges as vertices.
4. Every vertex of H has degree 2.

Note that if G contains only one vertex and G has a Hamiltonian circuit, then the circuit has the form $v\ e\ v$, where v is the vertex of G and e is an edge incident on v. In this case, the subgraph H consisting of v and e satisfies conditions (1)–(4) of Proposition 10.1.6.

Recall that the contrapositive of a statement is logically equivalent to the statement. The contrapositive of Proposition 10.1.6 says that if a graph G does *not* have a subgraph H with properties (1)–(4), then G does *not* have a Hamiltonian circuit.

Example 10.1.9 **Showing That a Graph Does Not Have a Hamiltonian Circuit**

Prove that the graph G shown below does not have a Hamiltonian circuit.



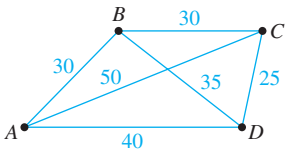
Solution If G has a Hamiltonian circuit, then by Proposition 10.1.6, G has a subgraph H that (1) contains every vertex of G, (2) is connected, (3) has the same number of edges as vertices, and (4) is such that every vertex has degree 2. Suppose such a subgraph H exists.

In other words, suppose there is a connected subgraph H of G such that H has five vertices (a, b, c, d, e) and five edges and such that every vertex of H has degree 2. Since the degree of b in G is 4 and every vertex of H has degree 2, two edges incident on b must be removed from G to create H. Edge $\{a, b\}$ cannot be removed because if it were, vertex a would have degree less than 2 in H. Similar reasoning shows that edges $\{e, b\}$, $\{b, a\}$, and $\{b, d\}$ cannot be removed either. It follows that the degree of b in H must be 4, which contradicts the condition that every vertex in H has degree 2 in H. Hence no such subgraph H exists, and so G does not have a Hamiltonian circuit. ■

The next example illustrates a type of problem known as a **traveling salesman problem**. It is a variation of the problem of finding a Hamiltonian circuit for a graph.

Example 10.1.10 **A Traveling Salesman Problem**

Imagine that the drawing below is a map showing four cities and the distances in kilometers between them. Suppose that a salesman must travel to each city exactly once, starting and ending in city A. Which route from city to city will minimize the total distance that must be traveled?



Solution This problem can be solved by writing all possible Hamiltonian circuits starting and ending at A and calculating the total distance traveled for each.

Route	Total Distance (In Kilometers)	
$A\ B\ C\ D\ A$	$30 + 30 + 25 + 40 = 125$	
$A\ B\ D\ C\ A$	$30 + 35 + 25 + 50 = 140$	
$A\ C\ B\ D\ A$	$50 + 30 + 35 + 40 = 155$	
$A\ C\ D\ B\ A$	140	[$A\ B\ D\ C\ A$ backward]
$A\ D\ B\ C\ A$	155	[$A\ C\ B\ D\ A$ backward]
$A\ D\ C\ B\ A$	125	[$A\ B\ C\ D\ A$ backward]

Thus either route $A\ B\ C\ D\ A$ or $A\ D\ C\ B\ A$ gives a minimum total distance of 125 kilometers. ■

The general traveling salesman problem involves finding a Hamiltonian circuit to minimize the total distance traveled for an arbitrary graph with n vertices in which each edge is marked with a distance. One way to solve the general problem is to use the method of Example 10.1.10: Write down all Hamiltonian circuits starting and ending at a particular vertex, compute the total distance for each, and pick one for which this total is minimal. However, even for medium-sized values of n this method is impractical. For a complete graph with 30 vertices, it would be necessary to check $(29!)/2 \cong 4.42 \times 10^{30}$ Hamiltonian circuits that start and end at a particular vertex. Even if each circuit could be found and its total distance computed in just one nanosecond, it would require approximately 1.4×10^{14} years to finish the computation. At present, there is no known algorithm for solving the general traveling salesman problem that is more efficient. However, there are efficient algorithms that find "pretty good" solutions—that is, circuits that, while not necessarily having the least possible total distances, have smaller total distances than most other Hamiltonian circuits.

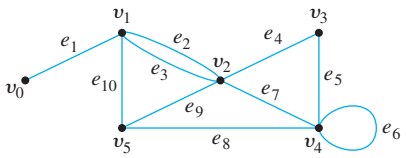
TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

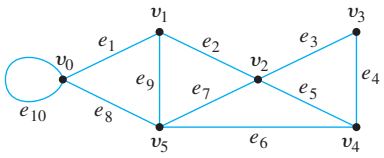
1. Let G be a graph and let v and w be vertices in G.
   (a) A walk from v to w is _____.
   (b) A trail from v to w is _____.
   (c) A path from v to w is _____.
   (d) A closed walk is _____.
   (e) A circuit is _____.
   (f) A simple circuit is _____.
   (g) A trivial walk is _____.
   (h) Vertices v and w are connected if, and only if, _____.
2. A graph is connected if, any only if, _____.
3. Removing an edge from a circuit in a graph does not _____.
4. An Euler circuit in a graph is _____.
5. A graph has a Euler circuit if, and only if, _____.
6. Given vertices v and w in a graph, there is an Euler trail from v to w if, and only if, _____.
7. A Hamiltonian circuit in a graph is _____.
8. If a graph G has a Hamiltonian circuit, then G has a subgraph H with the following properties: _____, _____, _____, and _____.
9. A traveling salesman problem involves finding a _____ that minimizes the total distance traveled for a graph in which each edge is marked with a distance.

EXERCISE SET 10.1*

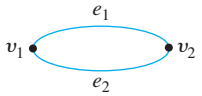
1. In the graph below, determine whether the following walks are trails, paths, closed walks, circuits, simple circuits, or just walks.
   a. $v_0e_1v_1e_{10}v_5e_9v_2e_2v_1$ **b.** $v_4e_7v_2e_9v_5e_{10}v_1e_3v_2e_9v_5$
   c. v_2 **d.** $v_5v_2v_3v_4v_4v_5$
   e. $v_2v_3v_4v_5v_2v_4v_3v_2$ **f.** $e_5e_8e_{10}e_3$



2. In the graph below, determine whether the following walks are trails, paths, closed walks, circuits, simple circuits, or just walks.
   a. $v_1e_2v_2e_3v_3e_4v_4e_5v_2e_2v_1e_1v_0$ **b.** $v_2v_3v_4v_5v_2$
   c. $v_4v_2v_3v_4v_5v_2v_4$ **d.** $v_2v_1v_5v_2v_3v_4v_2$
   e. $v_0v_5v_2v_3v_4v_2v_1$ **f.** $v_5v_4v_2v_1$

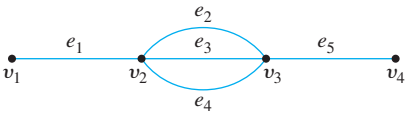


3. Let G be the graph



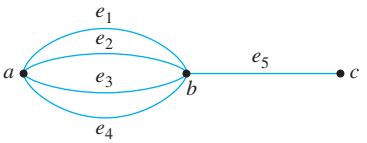
   and consider the walk $v_1e_1v_2e_2v_1$.
   a. Can this walk be written unambiguously as $v_1v_2v_1$? Why?
   b. Can this walk be written unambiguously as e_1e_2? Why?

4. Consider the following graph.



   a. How many paths are there from v_1 to v_4?
   b. How many trails are there from v_1 to v_4?
   c. How many walks are there from v_1 to v_4?

5. Consider the following graph.

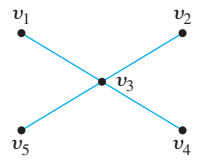


   a. How many paths are there from a to c?
   b. How many trails are there from a to c?
   c. How many walks are there from a to c?

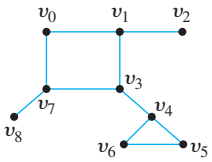
6. An edge whose removal disconnects the graph of which it is a part is called a **bridge**. Find all bridges for each of the graphs at the top of the next page.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

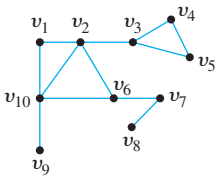
a.



b.



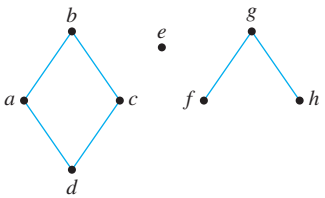
c.



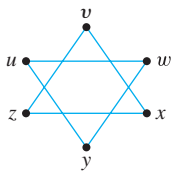
7. Given any positive integer n, (a) find a connected graph with n edges such that removal of just one edge disconnects the graph; (b) find a connected graph with n edges that cannot be disconnected by the removal of any single edge.

8. Find the number of connected components for each of the following graphs.

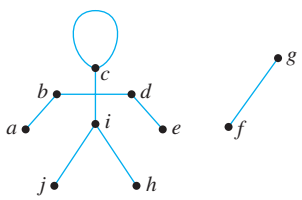
a.



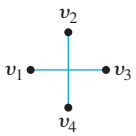
b.



c.



d.



9. Each of (a)–(c) describes a graph. In each case answer *yes*, *no*, or *not necessarily* to this question: Does the graph have an Euler circuit? Justify your answers.

a. G is a connected graph with five vertices of degrees 2, 2, 3, 3, and 4.

b. G is a connected graph with five vertices of degrees 2, 2, 4, 4, and 6.

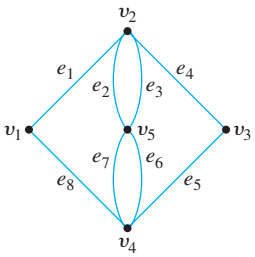
c. G is a graph with five vertices of degrees 2, 2, 4, 4, and 6.

10. The solution for Example 10.1.6 shows a graph for which every vertex has even degree but which does not have an Euler circuit. Give another example of a graph satisfying these conditions.

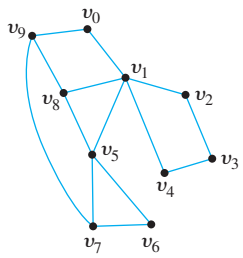
11. Is it possible for a citizen of Königsberg to make a tour of the city and cross each bridge exactly twice? (See Figure 10.1.1.) Explain.

Determine which of the graphs in 12–17 have Euler circuits. If the graph does not have an Euler circuit, explain why not. If it does have an Euler circuit, describe one.

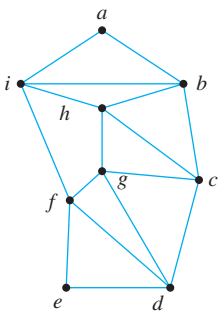
12.



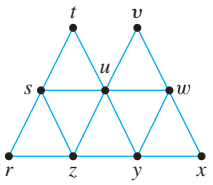
13.



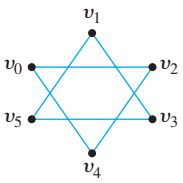
14.



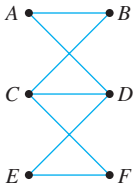
15.



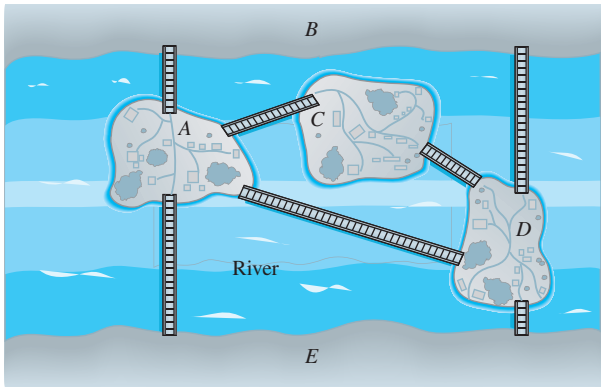
16.



17.

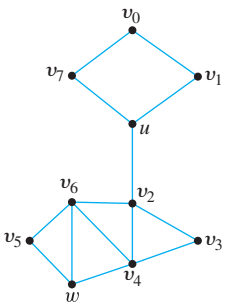


18. Is it possible to take a walk around the city whose map is shown below, starting and ending at the same point and crossing each bridge exactly once? If so, how can this be done?

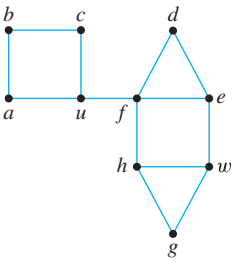


For each of the graphs in 19–21, determine whether there is an Euler trial from u to w. If there is, find such a trail.

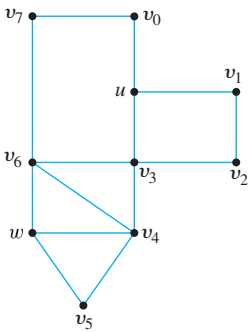
19.



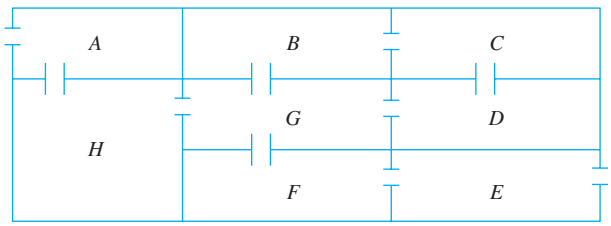
20.



21.

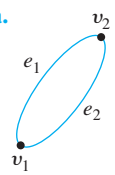


22. The following is a floor plan of a house. Is it possible to enter the house in room A, travel through every interior doorway of the house exactly once, and exit out of room E? If so, how can this be done?

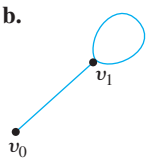


23. Find all subgraphs of each of the following graphs.

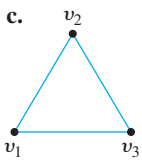
a.



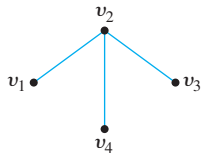
b.



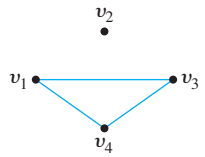
c.



Definition: If G is a simple graph, the **complement of G, denoted G'**, is obtained as follows: The vertex set of G' is identical to the vertex set of G. However, two distinct vertices v and w of G' are connected by an edge if, and only if, v and w are not connected by an edge in G. For example, if G is the graph

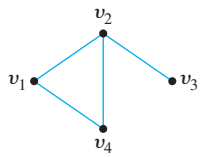


then G' is

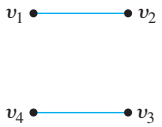


24. Find the complement of each of the following graphs.

a.



b.



25. **a.** Find the complement of the graph K_4, the complete graph on four vertices.

b. Find the complement of the graph $K_{3,2}$, the complete bipartite graph on (3, 2) vertices.

26. Suppose that in a group of five people A, B, C, D, and E the following pairs of people are acquainted with each other.

A and C, A and D, B and C, C and D, C and E.

a. Draw a graph to represent this situation.

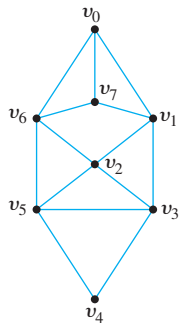
b. Draw a graph that illustrates who among these five people are *not* acquainted. That is, draw an edge between two people if, and only if, they are not acquainted.

***H* 27.** Let G be a simple graph with n vertices. What is the relation between the number of edges of G and the number of edges of the complement G'?

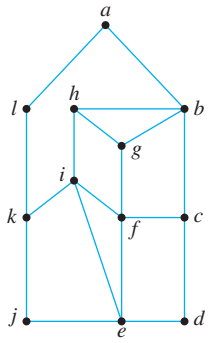
28. Show that at a party with at least two people, there are at least two mutual acquaintances or at least two mutual strangers.

Find Hamiltonian circuits for each of the graphs in 29 and 30.

29.

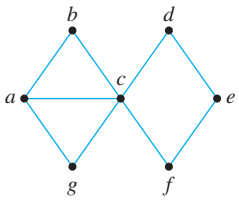


30.

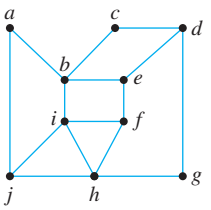


Show that none of the graphs in 31–33 has a Hamiltonian circuit.

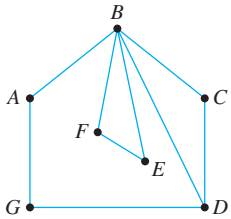
***H* 31.**



32.

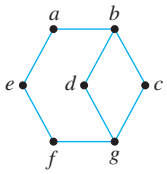


33.

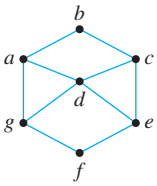


In 34–37, find Hamiltonian circuits for those graphs that have them. Explain why the other graphs do not.

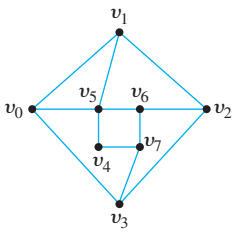
***H* 34.**



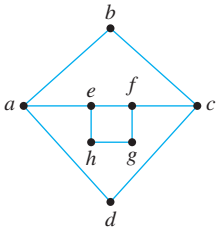
35.



36.



37.



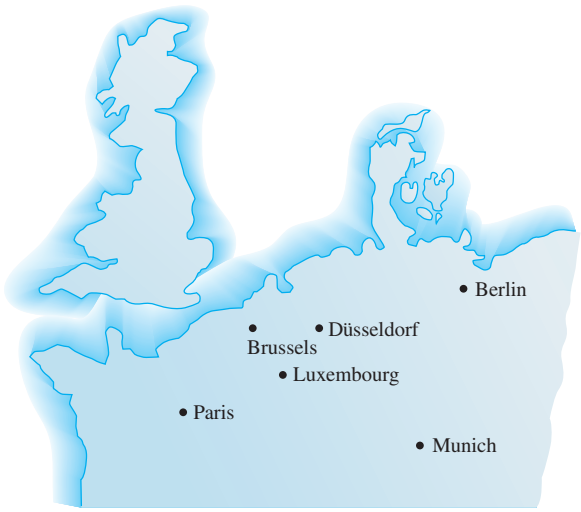
***H* 38.** Give two examples of graphs that have Euler circuits but not Hamiltonian circuits.

***H* 39.** Give two examples of graphs that have Hamiltonian circuits but not Euler circuits.

***H* 40.** Give two examples of graphs that have circuits that are both Euler circuits and Hamiltonian circuits.

***H* 41.** Give two examples of graphs that have Euler circuits and Hamiltonian circuits that are not the same.

42. A traveler in Europe wants to visit each of the cities shown on the map exactly once, starting and ending in Brussels. The distance (in kilometers) between each pair of cities is given in the table. Find a Hamiltonian circuit that minimizes the total distance traveled. (Use the map to narrow the possible circuits down to just a few. Then use the table to find the total distance for each of those.)



	Berlin	Brussels	Düsseldorf	Luxembourg	Munich
Brussels	783				
Düsseldorf	564	223			
Luxembourg	764	219	224		
Munich	585	771	613	517	
Paris	1,057	308	497	375	832

43. a. Prove that if a walk in a graph contains a repeated edge, then the walk contains a repeated vertex.

b. Explain how it follows from part (a) that any walk with no repeated vertex has no repeated edge.

44. Prove Lemma 10.1.1(a): If G is a connected graph, then any two distinct vertices of G can be connected by a path. (You may use the result stated in exercise 43.)

45. Prove Lemma 10.1.1(b): If vertices v and w are part of a circuit in a graph G and one edge is removed from the circuit, then there still exists a trail from v to w in G.

46. Draw a picture to illustrate Lemma 10.1.1(c): If a graph G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.

47. Prove that if there is a trail in a graph G from a vertex v to a vertex w, then there is a trail from w to v.

***H* 48.** If a graph contains a circuit that starts and ends at a vertex v, does the graph contain a simple circuit that starts and ends at v? Why?

49. Prove that if there is a circuit in a graph that starts and ends at a vertex v and if w is another vertex in the circuit, then there is a circuit in the graph that starts and ends at w.

50. Let G be a connected graph, and let C be any circuit in G that does not contain every vertex of C. Let G' be the subgraph obtained by removing all the edges of C from G and also any vertices that become isolated when the edges of C are removed. Prove that there exists a vertex v such that v is in both C and G'.

51. Prove that any graph with an Euler circuit is connected.

52. Prove Corollary 10.1.5.

53. For what values of n does the complete graph K_n with n vertices have (a) an Euler circuit? (b) a Hamiltonian circuit? Justify your answers.

*** 54.** For what values of m and n does the complete bipartite graph on (m, n) vertices have (a) an Euler circuit? (b) a Hamiltonian circuit? Justify your answers.

*** 55.** What is the maximum number of edges a simple disconnected graph with n vertices can have? Prove your answer.

***H* 56.** **a.** Prove that if G is any bipartite graph, then every circuit in G has an even number of edges.
b. Prove that if G is any graph with at least two vertices and if G does not have a circuit with an odd number of edges, then G is bipartite.

57. An alternative proof for Theorem 10.1.3 has the following outline. Suppose G is a connected graph in which every vertex has even degree. Suppose the path C: $v_1e_1v_2e_2v_3 \ldots e_nv_{n+1}$ has maximum length in G. That is, C has at least as many vertices and edges as any other path in G. First derive a contradiction from the assumption that $v_1 \neq v_n$. Next let H be the subgraph of G that contains all the vertices and edges in C. Then derive a contraction from the assumption that $H \neq G$. Show that H contains every vertex of G, and show that H contains every edge of G.

ANSWERS FOR TEST YOURSELF

1. (a) a finite alternating sequence of adjacent vertices and edges of G (b) a walk that does not contain a repeated edge (c) a trail that does not contain a repeated vertex (d) a walk that starts and ends at the same vertex (e) a closed walk that contains at least one edge and does not contain a repeated edge (f) a circuit that does not have any repeated vertex other than the first and the last (g) a walk consisting of a single vertex and no edge (h) there is a walk from v to w **2.** given any two vertices in the graph, there is a walk from one to the other **3.** disconnect the graph **4.** a circuit that contains every vertex and every edge of the graph **5.** the graph is connected, and every vertex has positive, even degree **6.** the graph is connected, v and w have odd degree, and all other vertices have positive even degree **7.** a simple circuit that includes every vertex of the graph **8.** H contains every vertex of G; H is connected; H has the same number of edges as vertices; every vertex of H has degree 2 **9.** Hamiltonian circuit

10.2 Matrix Representations of Graphs

Order and simplification are the first steps toward the mastery of a subject.
—Thomas Mann, *The Magic Mountain*, 1924

How can graphs be represented inside a computer? It happens that all the information needed to specify a graph can be conveyed by a structure called a *matrix*, and matrices (*matrices* is the plural of *matrix*) are easy to represent inside computers. This section contains some basic definitions about matrices and matrix operations, a description of the relation between graphs and matrices, and some applications.

Matrices

Matrices are two-dimensional analogues of sequences. They are also called two-dimensional arrays.

Definition

An $m \times n$ (read "m by n") **matrix A over a set S** is a rectangular array of elements of S arranged into m rows and n columns:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix} \leftarrow i\text{th row of } \mathbf{A}$$

$$\uparrow$$
$$j\text{th column of } \mathbf{A}$$

We write $\mathbf{A} = (a_{ij})$.

The ***i*th row of A** is

$$[a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}]$$

and the ***j*th column of A** is

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

The entry a_{ij} in the ith row and jth column of **A** is called the ***ij*th entry of A**. An $m \times n$ matrix is said to have **size $m \times n$**. If **A** and **B** are matrices, then **A = B** if, and only if, **A** and **B** have the same size and the corresponding entries of **A** and **B** are all equal; that is,

$$a_{ij} = b_{ij} \quad \text{for every } i = 1, 2, \ldots, m \text{ and } j = 1, 2, \ldots, n.$$

A matrix for which the numbers of rows and columns are equal is called a **square matrix**. If **A** is a square matrix of size $n \times n$, then the **main diagonal of A** consists of all the entries $a_{11}, a_{22}, \ldots, a_{nn}$:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1i} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2i} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{ni} & \cdots & a_{nn} \end{bmatrix}$$

main diagonal of **A**

Example 10.2.1 **Matrix Terminology**

The following is a 3×3 matrix over the set of integers.

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & -3 \\ 4 & -1 & 5 \\ -2 & 2 & 0 \end{bmatrix}$$

a. What is a_{23}, the entry in row 2, column 3?

b. What is the second column of **A**?

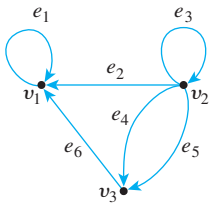
c. What are the entries in the main diagonal of **A**?

Solution

a. $a_{23} = 5$ b. $\begin{bmatrix} 0 \\ -1 \\ 2 \end{bmatrix}$ c. 1, −1, and 0 ■

Matrices and Directed Graphs

Consider the directed graph shown in Figure 10.2.1. This graph can be represented by the matrix $\mathbf{A} = (a_{ij})$ for which a_{ij} = the number of arrows from v_i to v_j, for every $i = 1, 2, 3$ and $j = 1, 2, 3$. Thus $a_{11} = 1$ because there is one arrow from v_1 to v_1; $a_{12} = 0$ because there is no arrow from v_1 to v_2, $a_{23} = 2$ because there are two arrows from v_2 to v_3, and so forth. **A** is called the *adjacency matrix* of the directed graph. For convenient reference, the rows and columns of **A** are often labeled with the vertices of the graph G.



Directed Graph G

(a)

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

Adjacency Matrix of G

(b)

FIGURE 10.2.1 A Directed Graph and Its Adjacency Matrix

Definition

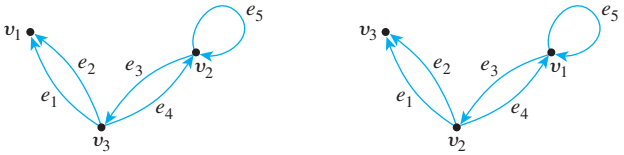
Let G be a directed graph with ordered vertices $v_1, v_2, \ldots, v_n$. The **adjacency matrix of G** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of nonnegative integers such that

$$a_{ij} = \text{the number of arrows from } v_i \text{ to } v_j \quad \text{for all } i, j = 1, 2, \ldots, n.$$

Note that nonzero entries along the main diagonal of an adjacency matrix indicate the presence of loops, and off-diagonal entries larger than 1 correspond to parallel edges. Moreover, if the vertices of a directed graph are reordered, then the entries in the rows and columns of the corresponding adjacency matrix are moved around.

Example 10.2.2 The Adjacency Matrix of a Graph

The two directed graphs shown below differ only in the ordering of their vertices. Find their adjacency matrices.



Solution Since both graphs have three vertices, both adjacency matrices are 3×3 matrices. For (a), all entries in the first row are 0 since there are no arrows from v_1 to any other vertex. For (b), the first two entries in the first row are 1 and the third entry is 0 since from v_1 there are single arrows to v_1 and to v_2 and no arrows to v_3. Continuing the analysis in this way, you obtain the following two adjacency matrices:

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 2 & 1 & 0 \end{bmatrix} \end{array} \qquad \text{(a)}$$

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \qquad \text{(b)}$$

■

If you are given a square matrix with nonnegative integer entries, you can construct a directed graph with that matrix as its adjacency matrix. However, the matrix does not tell you how to label the edges, so the directed graph is not uniquely determined.

Example 10.2.3 Obtaining a Directed Graph from a Matrix

Let

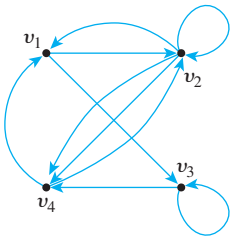
$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{bmatrix}.$$

Draw a directed graph that has $\mathbf{A}$ as its adjacency matrix.

Solution Let G be the graph corresponding to $\mathbf{A}$, and let v_1, v_2, v_3, and v_4 be the vertices of G. Label $\mathbf{A}$ across the top and down the left side with these vertex names, as shown below.

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Then, for instance, the 2 in the fourth row and the first column means that there are two arrows from v_4 to v_1. The 0 in the first row and the fourth column means that there is no arrow from v_1 to v_4. A corresponding directed graph is shown on the next page (without edge labels because the matrix does not determine those).



Matrices and Undirected Graphs

Once you know how to associate a matrix with a directed graph, the definition of the matrix corresponding to an undirected graph should seem natural to you. As before, you must order the vertices of the graph, but in this case you simply set the ijth entry of the adjacency matrix equal to the number of edges connecting the ith and jth vertices of the graph.

Definition

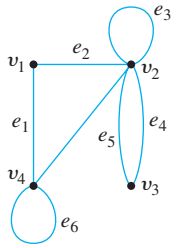
Let G be an undirected graph with ordered vertices $v_1, v_2, \ldots, v_n$. The **adjacency matrix of G** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of nonnegative integers such that

$$a_{ij} = \text{the number of edges connecting } v_i \text{ and } v_j$$

for every i and $j = 1, 2, \ldots, n$.

Example 10.2.4 **Finding the Adjacency Matrix of a Graph**

Find the adjacency matrix for the graph G shown below.



Solution

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

The entries of $\mathbf{A}$ satisfy the condition, $a_{ij} = a_{ji}$, for every $i, j = 1, 2, \ldots, n$. This implies that the appearance of $\mathbf{A}$ remains the same if the entries of $\mathbf{A}$ are flipped across its main diagonal. A matrix, like $\mathbf{A}$, with this property is said to be *symmetric*.

Definition

An $n \times n$ square matrix $\mathbf{A} = (a_{ij})$ is called **symmetric** if, and only if, for every i and $j = 1, 2, \ldots, n$,

$$a_{ij} = a_{ji}.$$

Example 10.2.5 **Symmetric Matrices**

Which of the following matrices are symmetric?

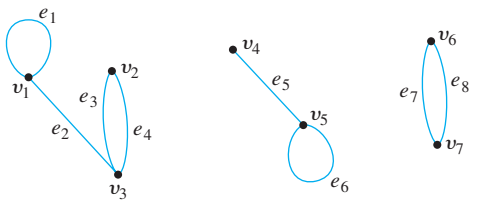
a. $\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$ b. $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 0 \\ 2 & 0 & 3 \end{bmatrix}$ c. $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

Solution Only (b) is symmetric. In (a) the entry in the first row and the second column differs from the entry in the second row and the first column; the matrix in (c) is not even square. ■

It is easy to see that the matrix of *any* undirected graph is symmetric since it is always the case that the number of edges joining v_i and v_j equals the number of edges joining v_j and v_i for every i and $j = 1, 2, \ldots, n$.

Matrices and Connected Components

Consider a graph G, as shown below, that consists of several connected components.



The adjacency matrix of G is

$$\mathbf{A} = \left[\begin{array}{ccc:c:cc} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{array}\right]$$

As you can see, $\mathbf{A}$ consists of square matrix blocks (of different sizes) down its diagonal and blocks of 0's everywhere else. The reason is that vertices in each connected component share no edges with vertices in other connected components. For instance, since v_1, v_2, and v_3 share no edges with v_4, v_5, v_6, or v_7, all entries in the top three rows to the right of the third column are 0 and all entries in the left three columns below the third row are also 0. Sometimes matrices whose entries are all 0's are themselves denoted 0. If this convention is followed here, $\mathbf{A}$ is written as

$$\mathbf{A} = \left[\begin{array}{ccc:c:cc} 1 & 0 & 1 & & & \\ 0 & 0 & 2 & & & \\ 1 & 2 & 0 & & & \\ \hdashline & & & 0 & 1 & \\ & 0 & & 1 & 1 & \\ \hdashline & & & & & 0 \quad 2 \\ & 0 & & & & 2 \quad 0 \end{array}\right]$$

The previous reasoning can be generalized to prove the following theorem:

Theorem 10.2.1

Let G be a graph with connected components $G_1, G_2, \ldots, G_k$. If there are n_i vertices in each connected component G_i and these vertices are numbered consecutively, then the adjacency matrix of G has the form

$$\begin{bmatrix} A_1 & \mathrm{O} & \mathrm{O} & \cdots & \mathrm{O} & \mathrm{O} \\ \mathrm{O} & A_2 & \mathrm{O} & \cdots & \mathrm{O} & \mathrm{O} \\ \mathrm{O} & \mathrm{O} & A_3 & \cdots & \mathrm{O} & \mathrm{O} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \cdots & \mathrm{O} & A_k \end{bmatrix}$$

where each A_i is the $n_i \times n_i$ adjacency matrix of G_i, for every $i = 1, 2, \ldots, k$, and the O's represent matrices whose entries are all 0.

Matrix Multiplication

Matrix multiplication is an enormously useful operation that arises in many contexts, including the investigation of walks in graphs. Although matrix multiplication can be defined in quite abstract settings, the definition for matrices whose entries are real numbers will be sufficient for our applications. The product of two matrices is built up of *scalar* or *dot* products of their individual rows and columns.

Definition

Suppose that all entries in matrices **A** and **B** are real numbers. If the number of element, n, in the ith row of **A** equals the number of elements in the jth column of **B**, then the **scalar product** or **dot product** of the ith row of **A** and jth column of **B** is the real number obtained as follows:

$$\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{bmatrix} \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Example 10.2.6 **Multiplying a Row and a Column**

$$\begin{bmatrix} 3 & 0 & -1 & 2 \end{bmatrix} \begin{bmatrix} -1 \\ 2 \\ 3 \\ 0 \end{bmatrix} = 3\cdot(-1) + 0\cdot 2 + (-1)\cdot 3 + 2\cdot 0$$

$$= -3 + 0 - 3 + 0 = -6$$ ■

More generally, if **A** and **B** are matrices whose entries are real numbers and if **A** and **B** have *compatible sizes* in the sense that the number of columns of **A** equals the number of rows of **B**, then the product **AB** is defined. It is the matrix whose ijth entry is the scalar product of the ith row of **A** times the jth column of **B**, for all possible values of i and j.

Definition

Let $\mathbf{A} = (a_{ij})$ be an $m \times k$ matrix and $\mathbf{B} = (b_{ij})$ a $k \times n$ matrix with real entries. The (matrix) product of $\mathbf{A}$ times $\mathbf{B}$, denoted $\mathbf{AB}$, is that matrix (c_{ij}) defined as follows:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix}$$

$$= \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{ij} & \cdots & c_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$

where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = \sum_{r=1}^{k} a_{ir}b_{rj},$$

for each $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

Example 10.2.7 **Computing a Matrix Product**

Let $\mathbf{A} = \begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix}$. Compute $\mathbf{AB}$.

Solution $\mathbf{A}$ has size 2×3 and $\mathbf{B}$ has size 3×2, so the number of columns of $\mathbf{A}$ equals the number of rows of $\mathbf{B}$ and the matrix product of $\mathbf{A}$ and $\mathbf{B}$ can be computed. Then

$$\begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix},$$

where

$$c_{11} = 2 \cdot 4 + 0 \cdot 2 + 3 \cdot (-2) = 2 \qquad \begin{bmatrix} \boxed{2} & \boxed{0} & \boxed{3} \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \boxed{4} & 3 \\ \boxed{2} & 2 \\ \boxed{-2} & -1 \end{bmatrix}$$

$$c_{12} = 2 \cdot 3 + 0 \cdot 2 + 3 \cdot (-1) = 3 \qquad \begin{bmatrix} \boxed{2} & \boxed{0} & \boxed{3} \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & \boxed{3} \\ 2 & \boxed{2} \\ -2 & \boxed{-1} \end{bmatrix}$$

$$c_{21} = (-1) \cdot 4 + 1 \cdot 2 + 0 \cdot (-2) = -2 \qquad \begin{bmatrix} 2 & 0 & 3 \\ \boxed{-1} & \boxed{1} & \boxed{0} \end{bmatrix} \begin{bmatrix} \boxed{4} & 3 \\ \boxed{2} & 2 \\ \boxed{-2} & -1 \end{bmatrix}$$

$$c_{22} = (-1) \cdot 3 + 1 \cdot 2 + 0 \cdot (-1) = -1 \qquad \begin{bmatrix} 2 & 0 & 3 \\ \boxed{-1} & \boxed{1} & \boxed{0} \end{bmatrix} \begin{bmatrix} 4 & \boxed{3} \\ 2 & \boxed{2} \\ -2 & \boxed{-1} \end{bmatrix}.$$

Hence

$$\mathbf{AB} = \begin{bmatrix} 2 & 3 \\ -2 & -1 \end{bmatrix}.$$

■

Matrix multiplication is both similar to and different from multiplication of real numbers. One difference is that although the product of any two numbers can be formed, only matrices with compatible sizes can be multiplied. For example, if **A** is a 3×2 matrix and **B** is a 2×4 matrix, then **AB** can be computed because the number of columns of **A** equals the number of rows of **B**. But **BA** does not exist because **B** has 4 columns, **A** has 3 rows, and $4 \neq 3$.

Another difference is that multiplication of real numbers is commutative (for all real numbers a and b, $ab = ba$), whereas matrix multiplication is not. For instance,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

On the other hand, both real number and matrix multiplications are associative: $(ab)c = a(bc)$, for all elements a, b, and c for which the products are defined. This is proved in Example 10.2.8 for products of 2×2 matrices. Additional exploration of matrix multiplication is offered in the exercises at the end of this section.

Example 10.2.8 **Associativity of Matrix Multiplication for 2×2 Matrices**

Prove that if **A**, **B**, and **C** are 2×2 matrices over the set of real numbers, then **(AB)C** = **A(BC)**.

Solution Suppose $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, and $\mathbf{C} = (c_{ij})$ are particular but arbitrarily chosen 2×2 matrices with real entries. Since the numbers of rows and columns are all the same, **AB**, **BC**, **(AB)C**, and **A(BC)** are defined. Let $\mathbf{AB} = (d_{ij})$ and $\mathbf{BC} = (e_{ij})$. Then for each integer $i = 1, 2$ and $j = 1, 2$,

$$\begin{aligned}
\text{the } ij\text{th entry of } \mathbf{(AB)C} &= \sum_{r=1}^{2} d_{ir}c_{rj} && \text{by definition of the product of } \mathbf{AB} \text{ and } \mathbf{C} \\
&= d_{i1}c_{1j} + d_{i2}c_{2j} && \text{by definition of } \Sigma \\
&= \left(\sum_{r=1}^{2} a_{ir}b_{r1}\right)c_{1j} + \left(\sum_{r=1}^{2} a_{ir}b_{r2}\right)c_{2j} && \text{by definition of the product of } \mathbf{A} \text{ and } \mathbf{B} \\
&= (a_{i1}b_{11} + a_{i2}b_{21})c_{1j} + (a_{i1}b_{12} + a_{i2}b_{22})c_{2j} && \text{by definition of } \Sigma \\
&= a_{i1}b_{11}c_{1j} + a_{i2}b_{21}c_{1j} + a_{i1}b_{12}c_{2j} + a_{i2}b_{22}c_{2j}.
\end{aligned}$$

Similarly, the ijth entry of **A(BC)** is

$$\begin{aligned}
(\mathbf{A(BC)})_{ij} &= \sum_{r=1}^{2} a_{ir}e_{rj} \\
&= a_{i1}e_{1j} + a_{i2}e_{2j} \\
&= a_{i1}\left(\sum_{r=1}^{2} b_{1r}c_{rj}\right) + a_{i2}\left(\sum_{r=1}^{2} b_{2r}c_{rj}\right) \\
&= a_{i1}(b_{11}c_{1j} + b_{12}c_{2j}) + a_{i2}(b_{21}c_{1j} + b_{22}c_{2j}) \\
&= a_{i1}b_{11}c_{1j} + a_{i1}b_{12}c_{2j} + a_{i2}b_{21}c_{1j} + a_{i2}b_{22}c_{2j} \\
&= a_{i1}b_{11}c_{1j} + a_{i2}b_{21}c_{1j} + a_{i1}b_{12}c_{2j} + a_{i2}b_{22}c_{2j}.
\end{aligned}$$

Comparing the results of the two computations shows that for each i and j,

$$\text{the } ij\text{th entry of } \mathbf{(AB)C} = \text{the } ij\text{th entry of } \mathbf{A(BC)}.$$

Since all corresponding entries are equal, $\mathbf{(AB)C} = \mathbf{A(BC)}$, as was to be shown. ■

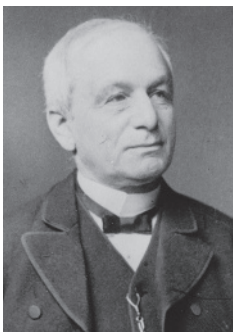
As far as multiplicative identities are concerned, there are both similarities and differences between real numbers and matrices. You know that the number 1 acts as a multiplicative identity for products of real numbers. It turns out that there are certain matrices, called *identity matrices*, that act as multiplicative identities for certain matrix products. For instance, mentally perform the following matrix multiplications to check that for any real numbers a, b, c, d, e, f, g, h, and i,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$

and

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}.$$

These computations show that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ acts as an identity on the left side for multiplication with 2×3 matrices and that $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ acts as an identity on the left side for multiplication with 3×3 matrices. Note that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ cannot act as an identity on the right side for multiplication with 2×3 matrices because the sizes are not compatible.



akg-images/akg-images

Leopold Kronecker (1823–1891)

Definition

For each positive integer n, the $\boldsymbol{n \times n}$ **identity matrix**, denoted $\mathbf{I}_n = (\boldsymbol{\delta}_{ij})$ or just $\mathbf{I}$ (if the size of the matrix is obvious from context), is the $n \times n$ matrix in which all the entries in the main diagonal are 1's and all other entries are 0's. In other words,

$$\delta_{ij} = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases}, \quad \text{for every } i, j = 1, 2, \ldots, n.$$

The German mathematician Leopold Kronecker introduced the symbol δ_{ij} to make matrix computations more convenient. In his honor, this symbol is called the *Kronecker delta*.

Example 10.2.9 **An Identity Matrix Acts as an Identity**

Prove that if $\mathbf{A}$ is any $m \times n$ matrix and $\mathbf{I}$ is the $n \times n$ identity matrix, then $\mathbf{AI} = \mathbf{A}$.

Proof:

Let $\mathbf{A}$ be any $n \times n$ matrix and let a_{ij} be the ijth entry of $\mathbf{A}$ for each integer $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. Consider the product $\mathbf{AI}$, where $\mathbf{I}$ is the $n \times n$ identity matrix. Observe that

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

because

$$\begin{aligned} \text{the } ij\text{th entry of } \mathbf{AI} &= \sum_{r=1}^{n} a_{ir}\delta_{rj} && \text{by definition of 1} \\ &= a_{i1}\delta_{1j} + a_{i2}\delta_{2j} + \cdots && \text{by definition of } \Sigma \\ &\quad + a_{ij}\delta_{jj} + \cdots + a_{in}\delta_{nj} \\ &= a_{ij}\delta_{jj} && \text{since } \delta_{kj} = 0 \text{ whenever } k \neq j \\ &= a_{ij} && \text{since } \delta_{jj} = 1 \\ &= \text{the } ij\text{th entry of } \mathbf{A}. \end{aligned}$$

Thus $\mathbf{AI} = \mathbf{A}$, as was to be shown. ■

In exercise 14 at the end of this section you are asked to show that if $\mathbf{I}$ is the $m \times m$ identity matrix, then $\mathbf{IA} = \mathbf{A}$.

There are also similarities and differences between real numbers and matrices with respect to the computation of powers. Any number can be raised to a nonnegative integer power, but a matrix can be multiplied by itself only if it has the same number of rows as columns. As for real numbers, however, the definition of matrix powers is recursive. Just as any number to the zeroth power is defined to be 1, so any $n \times n$ matrix to the zeroth power is defined to be the $n \times n$ identity matrix. The nth power of an $n \times n$ matrix $\mathbf{A}$ is defined to be the product of $\mathbf{A}$ with its $(n-1)$st power.

Definition

For any $n \times n$ matrix $\mathbf{A}$, the powers of $\mathbf{A}$ are defined as follows:

$$\mathbf{A}^0 = \mathbf{I} \quad \text{where } \mathbf{I} \text{ is the } n \times n \text{ identity matrix}$$
$$\mathbf{A}^n = \mathbf{A}\mathbf{A}^{n-1} \quad \text{for every integer } n \geq 1.$$

Example 10.2.10 **Powers of a Matrix**

Let $\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}$. Compute $\mathbf{A}^0$, $\mathbf{A}^1$, $\mathbf{A}^2$, and $\mathbf{A}^3$.

Solution

$$\mathbf{A}^0 = \text{the } 2 \times 2 \text{ identity matrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\mathbf{A}^1 = \mathbf{A}\mathbf{A}^0 = \mathbf{A}\mathbf{I} = \mathbf{A}$$

$$\mathbf{A}^2 = \mathbf{A}\mathbf{A}^1 = \mathbf{A}\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix}$$

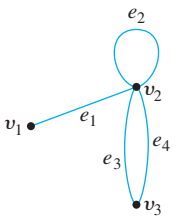
$$\mathbf{A}^3 = \mathbf{A}\mathbf{A}^2 = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 9 & 10 \\ 10 & 4 \end{bmatrix}$$

■

Counting Walks of Length N

A walk in a graph consists of an alternating sequence of vertices and edges. If repeated edges are counted each time they occur, then the number of edges in the sequence is called

the **length** of the walk. For instance, the walk $v_2e_3v_3e_4v_2e_2v_2e_3v_3$ has length 4 (counting e_3 twice). Consider the following graph G:



How many distinct walks of length 2 connect v_2 and v_2? You can list the possibilities systematically as follows: From v_1, the first edge of the walk must go to *some* vertex of G: v_1, v_2, or v_3. There is one walk of length 2 from v_2 to v_2 that starts by going from v_2 to v_1:

$$v_2e_1v_1e_1v_2.$$

There is one walk of length 2 from v_2 to v_2 that starts by going from v_2 to v_2:

$$v_2e_2v_2e_2v_2.$$

And there are four walks of length 2 from v_2 to v_2 that start by going from v_2 to v_3:

$$v_2e_3v_3e_4v_2$$
$$v_2e_4v_3e_3v_2$$
$$v_2e_3v_3e_3v_2$$
$$v_2e_4v_3e_4v_2.$$

Thus the answer is six.

The general question of finding the number of walks that have a given length and connect two particular vertices of a graph can easily be answered using matrix multiplication. Consider the adjacency matrix $\mathbf{A}$ of the graph G shown above:

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \end{array}.$$

Compute $\mathbf{A}^2$ as follows:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 6 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$$

Note that the entry in the second row and the second column is 6, which equals the number of walks of length 2 from v_2 to v_2. This is no accident! To compute a_{22}, you multiply the second row of $\mathbf{A}$ times the second column of $\mathbf{A}$ to obtain a sum of three terms:

$$\begin{bmatrix} 1 & 1 & 2 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} = 1\cdot 1 + 1\cdot 1 + 2\cdot 2.$$

Observe that

$$\begin{bmatrix} \text{the first term} \\ \text{of this sum} \end{bmatrix} = \begin{bmatrix} \text{number of} \\ \text{edges from} \\ v_2 \text{ to } v_1 \end{bmatrix} \cdot \begin{bmatrix} \text{number of} \\ \text{edges from} \\ v_1 \text{ to } v_2 \end{bmatrix} = \begin{bmatrix} \text{number of pairs} \\ \text{of edges from} \\ v_2 \text{ to } v_1 \text{ and } v_1 \text{ to } v_2 \end{bmatrix}.$$

Now consider the ith term of this sum, for each $i = 1$, 2, and 3. It equals the number of edges from v_2 to v_i times the number of edges from v_i to v_2. By the multiplication rule this equals the number of pairs of edges from v_2 to v_i and from v_i back to v_2. And this equals the number of walks of length 2 that start and end at v_2 and pass through v_i. Since this analysis holds for each term of the sum for $i = 1$, 2, and 3, the sum as a whole equals the total number of walks of length 2 that start and end at v_2:

$$1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 = 1 + 1 + 4 = 6.$$

More generally, if $\mathbf{A}$ is the adjacency matrix of a graph G, the ijth entry of $\mathbf{A}^2$ equals the number of walks of length 2 connecting the ith vertex to the jth vertex of G. Even more generally, if n is any positive integer, the ijth entry of $\mathbf{A}^n$ equals the number of walks of length n connecting the ith and the jth vertices of G.

Theorem 10.2.2

If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and $\mathbf{A}$ is the adjacency matrix of G, then for each positive integer n and for all integers $i, j = 1, 2, \ldots, m$,

$$\text{the } ij\text{th entry of } \mathbf{A}^n = \text{the number of walks of length } n \text{ from } v_i \text{ to } v_j.$$

Proof (by mathematical induction):

Suppose G is a graph with vertices $v_1, v_2, \ldots, v_m$ and $\mathbf{A}$ is the adjacency matrix of G. Let $P(n)$ be the sentence

For all integers $i, j = 1, 2, \ldots, m$, ← $P(n)$
the ijth entry of $\mathbf{A}^n$ = the number of walks of length n from v_i to v_j.

We will show that $P(n)$ is true for every integer $n \geq 1$.

Show that* P(1) *is true:

The ijth entry of $\mathbf{A}^1$ = the ijth entry of $\mathbf{A}$ — because $\mathbf{A}^1 = \mathbf{A}$
= the number of edges connecting v_i to v_j — by definition of adjacency matrix
= the number of walks of length 1 from v_i to v_j — because a walk of length 1 contains a single edge.

Show that for every integer k with k ≥ 1, if P(k) is true then P(k +1) is true:

Let k be any integer with $k \geq 1$, and suppose that

For all integers $i, j = 1, 2, \ldots, m$, ← $P(k)$
the ijth entry of $\mathbf{A}^k$ = the number of walks of length k from v_i to v_j — inductive hypothesis

We must show that

For all integers $i, j = 1, 2, \ldots, m$, ← $P(k+1)$
the ijth entry of $\mathbf{A}^{k+1}$ = the number of walks of length $k+1$ from v_i to v_j.

Let $\mathbf{A} = (a_{ij})$ and $\mathbf{A}^k = (b_{ij})$. Since $\mathbf{A}^{k+1} = \mathbf{A}\mathbf{A}^k$, the ijth entry of $\mathbf{A}^{k+1}$ is obtained by multiplying the ith row of $\mathbf{A}$ by the jth column of $\mathbf{A}^k$:

$$\text{the } ij\text{th entry of } \mathbf{A}^{k+1} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj} \qquad 10.2.1$$

for every $i, j = 1, 2, \ldots, m$. Now consider the individual terms of this sum: a_{i1} is the number of edges from v_i to v_1; and, by the inductive hypothesis, b_{1j} is the number of walks of length k from v_1 to v_j. Now any edge from v_i to v_1 can be joined with any

(continued on page 710)

walk of length k from v_1 to v_j to create a walk of length $k+1$ from v_i to v_j with v_1 as its second vertex. Thus, by the multiplication rule,

$$a_{i1}b_{1j} = \begin{bmatrix}\text{the number of walks of length } k+1 \text{ from} \\ v_i \text{ to } v_j \text{ that have } v_1 \text{ as their second vertex}\end{bmatrix}.$$

More generally, for each integer $r = 1, 2, \ldots, m$,

$$a_{ir}b_{rj} = \begin{bmatrix}\text{the number of walks of length } k+1 \text{ from} \\ v_i \text{ to } v_j \text{ that have } v_r \text{ as their second vertex}\end{bmatrix}.$$

Because every walk of length $k+1$ from v_i to v_j must have one of the vertices $v_1, v_2, \ldots, v_m$ as its second vertex, the total number of walks of length $k+1$ from v_i to v_j equals the sum in (10.2.1), which equals the ijth entry of $\mathbf{A}^{k+1}$. Hence

$$\text{the } ij\text{th entry of } \mathbf{A}^{k+1} = \text{the number of walks of length } k+1 \text{ from } v_i \text{ to } v_j$$

[as was to be shown].
[Since both the basis step and the inductive step have been proved, the sentence P(n) is true for every integer $n \geq 1$.]

TEST YOURSELF

1. In the adjacency matrix for a directed graph, the entry in the ith row and jth column is _____.
2. In the adjacency matrix for an undirected graph, the entry in the ith row and jth column is _____.
3. An $n \times n$ square matrix is called symmetric if, and only if, for all integers i and j from 1 to n, the entry in row _____ and column _____ equals the entry in row _____ and column _____.
4. The ijth entry in the product of two matrices $\mathbf{A}$ and $\mathbf{B}$ is obtained by multiplying row _____ of $\mathbf{A}$ by row _____ of $\mathbf{B}$.
5. In an $n \times n$ identity matrix, the entries on the main diagonal are all _____ and the off-diagonal entries are all _____.
6. If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and $\mathbf{A}$ is the adjacency matrix of G, then for each positive integer n and for all integers i and j with $i, j = 1, 2, \ldots, m$, the ijth entry of $\mathbf{A}^n$ = _____.

EXERCISE SET 10.2

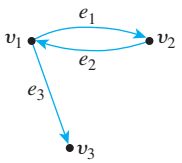
1. Find real numbers a, b, and c such that the following are true.

   a. $\begin{bmatrix} a+b & a-c \\ c & b-a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix}$

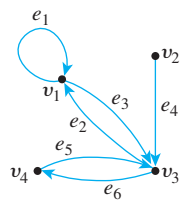
   b. $\begin{bmatrix} 2a & b+c \\ c-a & 2b-a \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 1 & -2 \end{bmatrix}$

2. Find the adjacency matrices for the following directed graphs.

a.



b.

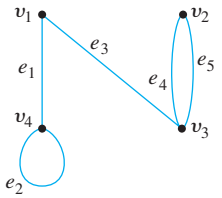


3. Find directed graphs that have the following adjacency matrices:

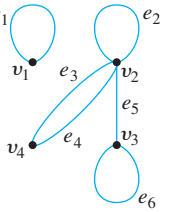
   a. $\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ **b.** $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

4. Find adjacency matrices for the following (undirected) graphs.

a.



b.



c. K_4, the complete graph on four vertices

d. $K_{2,3}$, the complete bipartite graph on (2, 3) vertices

5. Find graphs that have the following adjacency matrices.

a. $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$ **b.** $\begin{bmatrix} 0 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

6. The following are adjacency matrices for graphs. In each case determine whether the graph is connected by analyzing the matrix without drawing the graph.

a. $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ **b.** $\begin{bmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

7. Suppose that for every positive integer i, all the entries in the ith row and ith column of the adjacency matrix of a graph are 0. What can you conclude about the graph?

8. Find each of the following products.

a. $\begin{bmatrix} 2 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 3 \end{bmatrix}$ **b.** $\begin{bmatrix} 4 & -1 & 7 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$

9. Find each of the following products.

a. $\begin{bmatrix} 3 & 0 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 1 & -1 & 4 \\ 0 & 2 & 1 \end{bmatrix}$

b. $\begin{bmatrix} 2 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & -4 \\ -2 & 2 \end{bmatrix}$

c. $\begin{bmatrix} -1 \\ 2 \end{bmatrix}\begin{bmatrix} 2 & 3 \end{bmatrix}$

d. $\begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix}^2$

10. Let $\mathbf{A} = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -2 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -2 & 0 \\ 1 & 3 \end{bmatrix}$, and $\mathbf{C} = \begin{bmatrix} 0 & -2 \\ 3 & 1 \\ 1 & 0 \end{bmatrix}$.

For each of the following, determine whether the indicated product exists, and compute it if it does.

a. $\mathbf{AB}$ **b.** $\mathbf{BA}$ **c.** $\mathbf{A}^2$ **d.** $\mathbf{BC}$ **e.** $\mathbf{CB}$
f. $\mathbf{B}^2$ **g.** $\mathbf{B}^3$ **h.** $\mathbf{C}^2$ **i.** $\mathbf{AC}$ **j.** $\mathbf{CA}$

11. Give an example different from that in the text to show that matrix multiplication is not commutative. That is, find 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{AB}$ and $\mathbf{BA}$ both exist but $\mathbf{AB} \neq \mathbf{BA}$.

12. Let O denote the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Find 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A} \neq \mathrm{O}$ and $\mathbf{B} \neq \mathrm{O}$ but $\mathbf{AB} = \mathrm{O}$.

13. Let O denote the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Find 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A} \neq \mathbf{B}$, $\mathbf{B} \neq \mathrm{O}$, and $\mathbf{AB} \neq \mathrm{O}$, but $\mathbf{BA} = \mathrm{O}$.

In 14–18, assume the entries of all matrices are real numbers.

***H* 14.** Prove that if $\mathbf{I}$ is the $m \times m$ identity matrix and $\mathbf{A}$ is any $m \times n$ matrix, then $\mathbf{IA} = \mathbf{A}$.

15. Prove that if $\mathbf{A}$ is an $m \times m$ symmetric matrix, then $\mathbf{A}^2$ is symmetric.

16. Prove that matrix multiplication is associative: If $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ are any $m \times k$, $k \times r$, and $r \times n$ matrices, respectively, then $\mathbf{(AB)C} = \mathbf{A(BC)}$. (*Hint*: Summation notation is helpful.)

17. Use mathematical induction and the result of exercise 16 to prove that if $\mathbf{A}$ is any $m \times m$ matrix, then $\mathbf{A}^n\mathbf{A} = \mathbf{A}\mathbf{A}^n$ for each integer $n \geq 1$.

18. Use mathematical induction to prove that if $\mathbf{A}$ is an $m \times m$ symmetric matrix, then for any integer $n \geq 1$, $\mathbf{A}^n$ is also symmetric.

19. a. Let $\mathbf{A} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}$. Find $\mathbf{A}^2$ and $\mathbf{A}^3$.

b. Let G be the graph with vertices v_1, v_2, and v_3 and with $\mathbf{A}$ as its adjacency matrix. Use the answers to part (a) to find the number of walks of length 2 from v_1 to v_3 and the number of walks of length 3 from v_1 to v_3. Do not draw G to solve this problem.

c. Examine the calculations you performed in answering part (a) to find five walks of length 2 from v_3 to v_3. Then draw G and find the walks by visual inspection.

20. The following is an adjacency matrix for a graph:

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{array}$$

Answer the following questions by examining the matrix and its powers only, not by drawing the graph:

a. How many walks of length 2 are there from v_2 to v_3?

b. How many walks of length 2 are there from v_3 to v_4?

c. How many walks of length 3 are there from v_1 to v_4?

d. How many walks of length 3 are there from v_2 to v_3?

21. Let $\mathbf{A}$ be the adjacency matrix for K_3, the complete graph on three vertices. Use mathematical induction to prove that for each positive integer n, all the entries along the main diagonal of $\mathbf{A}^n$ are equal to each other and all the entries that do not lie along the main diagonal are equal to each other.

22. a. Draw a graph that has

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 1 & 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 \end{bmatrix}$$

as its adjacency matrix. Is this graph bipartite?

Definition: Given an $m \times n$ matrix $\mathbf{A}$ whose ijth entry is denoted a_{ij}, the **transpose of A** is the matrix $\mathbf{A}^t$ whose ijth entry is a_{ji}, for each $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

Note that the first row of $\mathbf{A}$ becomes the first column of $\mathbf{A}^t$, the second row of $\mathbf{A}$ becomes the second column of $\mathbf{A}^t$, and so forth. For instance,

$$\text{if } \mathbf{A} = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix}, \text{ then } \mathbf{A}^t = \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix}.$$

***H* b.** Show that a graph with n vertices is bipartite if, and only if, for some labeling of its vertices, its adjacency matrix has the form

$$\begin{bmatrix} \mathbf{O} & \mathbf{A} \\ \mathbf{A}^t & \mathbf{O} \end{bmatrix}$$

where $\mathbf{A}$ is a $k \times (n-k)$ matrix for some integer k such that $0 < k < n$, the top left O represents a $k \times k$ matrix all of whose entries are 0, $\mathbf{A}^t$ is the transpose of $\mathbf{A}$, and the bottom right O represents an $(n-k) \times (n-k)$ matrix all of whose entries are 0.

23. a. Let G be a graph with n vertices, and let v and w be distinct vertices of G. Prove that if there is a walk from v to w, then there is a walk from v to w that has length less than or equal to $n-1$.

***H* b.** If $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$ are any $m \times n$ matrices, the matrix $\mathbf{A} + \mathbf{B}$ is the $m \times n$ matrix whose ijth entry is $a_{ij} + b_{ij}$ for each $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. Let G be a graph with n vertices where $n > 1$, and let $\mathbf{A}$ be the adjacency matrix of G. Prove that G is connected if, and only if, every entry of $\mathbf{A} + \mathbf{A}^2 + \cdots + \mathbf{A}^{n-1}$ is positive.

ANSWERS FOR TEST YOURSELF

1. the number of arrows from v_i (the ith vertex) to v_j (the jth vertex) **2.** the number of edges connecting v_i (the ith vertex) and v_j (the jth vertex) **3.** i; j; j; i **4.** i; j **5.** 1; 0 **6.** the number of walks of length n from v_i to v_j

10.3 Isomorphisms of Graphs

Thinking is a momentary dismissal of irrelevancies. —R. Buckminster Fuller, 1969

The two drawings shown in Figure 10.3.1 both represent the same graph: Their vertex and edge sets are identical, and their edge-endpoint functions are the same. Call this graph G.

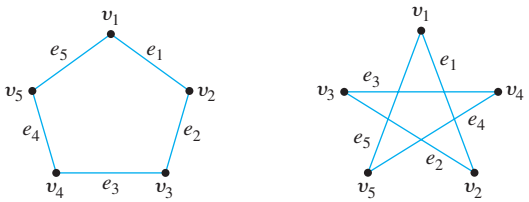


FIGURE 10.3.1

Now consider the graph G' represented in Figure 10.3.2.

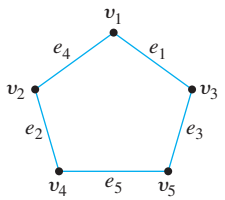


FIGURE 10.3.2

Observe that G' is a different graph from G (for instance, in G the endpoints of e_1 are v_1 and v_2, whereas in G' the endpoints of e_1 are v_1 and v_3). Yet G' is certainly very similar to G. In fact, if the vertices and edges of G' are relabeled by the functions shown in Figure 10.3.3, then G' becomes the same as G.

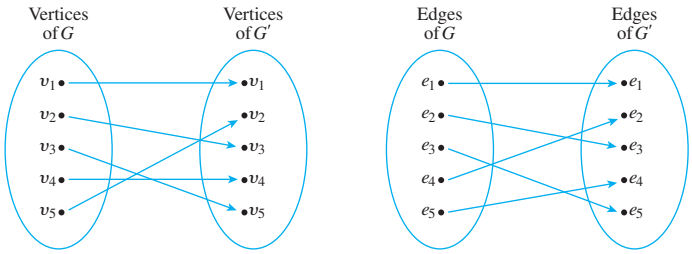


FIGURE 10.3.3

Note that these relabeling functions are one-to-one and onto.

Two graphs that are the same except for the labeling of their vertices and edges are called *isomorphic*. The word *isomorphism* comes from the Greek, meaning "same form." Isomorphic graphs are those that have essentially the same form.

Definition

Let G and G' be graphs with vertex sets $V(G)$ and $V(G')$ and edge sets $E(G)$ and $E(G')$, respectively. **G is isomorphic to G'** if, and only if, there exist one-to-one correspondences $g: V(G) \to V(G')$ and $h: E(G) \to E(G')$ that preserve the edge-endpoint functions of G and G' in the sense that for each $v \in V(G)$ and $e \in E(G)$,

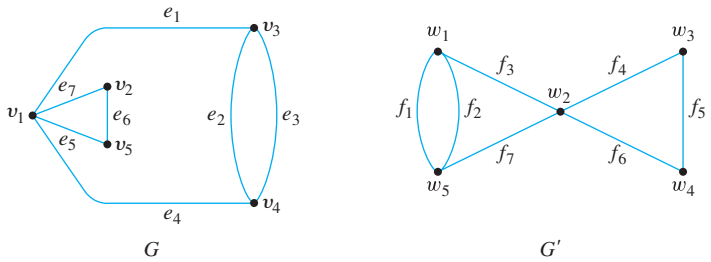
$$v \text{ is an endpoint of } e \iff g(v) \text{ is an endpoint of } h(e). \qquad 10.3.1$$

In words, G is isomorphic to G' if, and only if, the vertices and edges of G and G' can be matched up by one-to-one, onto functions in such a way that the edges between corresponding vertices correspond to each other.

It is common in mathematics to identify isomorphic objects with each other. For instance, if we are given a graph G with five vertices, where each pair of vertices is connected by an edge, then we often identify G with K_5, saying that G is K_5 rather than that G is isomorphic to K_5.

Example 10.3.1 **Showing That Two Graphs Are Isomorphic**

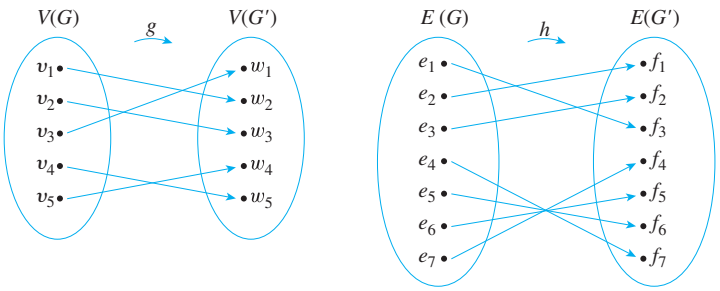
Show that the following two graphs are isomorphic.



Solution To solve this problem, you must find functions $g\colon V(G) \to V(G')$ and $h\colon E(G) \to E(G')$ such that for each $v \in V(G)$ and $e \in E(G)$, v is an endpoint of e if, and only if, $g(v)$ is an endpoint of $h(e)$. Setting up such functions is partly a matter of trial and error and partly a matter of deduction. For instance, since e_2 and e_3 are parallel *[have the same endpoints]*, $h(e_2)$ and $h(e_3)$ must be parallel also. So $h(e_2) = f_1$ and $h(e_3) = f_2$ or $h(e_2) = f_2$ and $h(e_3) = f_1$. Also, the endpoints of e_2 and e_3 must correspond to the endpoints of f_1 and f_2, and so $g(v_3) = w_1$ and $g(v_4) = w_5$ or $g(v_3) = w_5$ and $g(v_4) = w_1$.

Similarly, since v_1 is the endpoint of four distinct edges (e_1, e_7, e_5, and e_4), $g(v_1)$ must also be the endpoint of four distinct edges *[because every edge incident on $g(v_1)$ is the image under h of an edge incident on v_1 and h is one-to-one and onto]*. But the only vertex in G' that has four edges coming out of it is w_2, and so $g(v_1) = w_2$. Now if $g(v_3) = w_1$, then since v_1 and v_3 are endpoints of e_1 in G, $g(v_1) = w_2$ and $g(v_3) = w_1$ must be endpoints of $h(e_1)$ in G'. This implies that $h(e_1) = f_3$.

By continuing in this way, possibly making some arbitrary choices as you go, you eventually can find functions g and h to define the isomorphism between G and G'. One pair of functions (there are several) is the following:



■

It is not hard to show that graph isomorphism is an equivalence relation on a set of graphs; in other words, it is reflexive, symmetric, and transitive.

Theorem 10.3.1 Graph Isomorphism Is an Equivalence Relation

Let S be a set of graphs and let R be the relation of graph isomorphism on S. Then R is an equivalence relation on S.

Proof:

R is reflexive: Given any graph G in S, define a graph isomorphism from G to G by using the identity functions on the set of vertices and on the set of edges of G.

R is symmetric: Given any graphs G and G' in S such that G is isomorphic to G', we must show that G' is isomorphic to G.

This is true because if g and h are vertex and edge correspondences from G to G' that preserve the edge-endpoint functions, then g^{-1} and h^{-1} are vertex and edge correspondences from G' to G that preserve the edge-endpoint functions.

Note As a consequence of the symmetry property, you can simply say "G and G' are isomorphic" instead of "G is isomorphic to G'" or "G' is isomorphic to G."

R is transitive: Given any graphs G, G', and G'' in S such that G is isomorphic to G' and G' is isomorphic to G'', we must show that G is isomorphic to G''.

This follows from the fact that if g_1 and h_1 are vertex and edge correspondences from G to G' that preserve the edge-endpoint functions of G and G' and if g_2 and h_2 are vertex and edge correspondences from G' to G'' that preserve the edge-endpoint functions of G' and G'', then $g_2 \circ g_1$ and $h_2 \circ h_1$ are vertex and edge correspondences from G to G'' that preserve the edge-endpoint functions of G and G''.

Example 10.3.2 **Finding Representatives of Isomorphism Classes**

Find all nonisomorphic graphs that have two vertices and two edges. In other words, find a collection of representative graphs with two vertices and two edges such that every graph with two vertices and two edges is isomorphic to one in the collection.

Solution There are four nonisomorphic graphs that have two vertices and two edges. These can be drawn without vertex and edge labels because any two labelings give isomorphic graphs.

(a) (b) (c) (d)

To see that these four drawings show all the nonisomorphic graphs with two vertices and two edges, first check whether one of the edges joins the two vertices or not. If it does, there are two possibilities: The second edge can also join the two vertices (as in (a)) or it can be a loop incident on one of them (as in (b)—it makes no difference *which* vertex is chosen to have the loop because interchanging the two vertex labels gives isomorphic graphs). If neither edge joins the two vertices, then both edges are loops. In this case, there are only two possibilities: Either both loops are incident on the same vertex (as in (c)) or the two loops are incident on separate vertices (as in (d)). There are no other possibilities for placing the edges, so the listing is complete. ■

Now consider the question, "Is there a general method to determine whether graphs G and G' are isomorphic?" In other words, is there some algorithm that will accept graphs G and G' as input and produce a statement as to whether they are isomorphic? In fact, there is such an algorithm. It consists of generating all one-to-one, onto functions from the set of vertices of G to the set of vertices of G' and from the set of edges of G to the set of

edges of G' and checking each pair to determine whether it preserves the edge-endpoint functions of G and G'. The problem with this algorithm is that it takes an unreasonably long time to perform, even on a high-speed computer. If G and G' each have n vertices and m edges, the number of one-to-one correspondences from vertices to vertices is $n!$ and the number of one-to-one correspondences from edges to edges is $m!$, so the total number of pairs of functions to check is $n! \cdot m!$. For instance, if $m = n = 20$, there would be $20! \cdot 20! \cong 5.9 \times 10^{36}$ pairs to check. Assuming that each check takes just 1 nanosecond, the total time would be approximately 1.9×10^{20} years!

Unfortunately, there is no more efficient general method known for checking whether two graphs are isomorphic. However, there are some simple tests that can be used to show that certain pairs of graphs are *not* isomorphic. For instance, if two graphs are isomorphic, then they have the same number of vertices (because there is a one-to-one correspondence from the vertex set of one graph to the vertex set of the other). It follows that if you are given two graphs, one with 16 vertices and the other with 17, you can immediately conclude that the two are not isomorphic. More generally, a property that is preserved by graph isomorphism is called an *isomorphic invariant*. For instance, "having 16 vertices" is an isomorphic invariant: If one graph has 16 vertices, then so does any graph that is isomorphic to it.

Definition

A property P is called an **invariant for graph isomorphism** if, and only if, given any graphs G and G', if G has property P and G' is isomorphic to G, then G' has property P.

Theorem 10.3.2

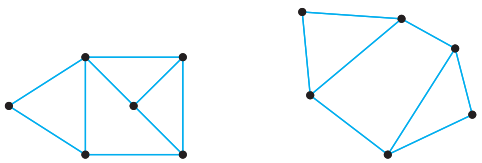
Each of the following properties is an invariant for graph isomorphism, where n, m, and k are all nonnegative integers:

1. has n vertices
2. has m edges
3. has a vertex of degree k
4. has m vertices of degree k
5. has a circuit of length k
6. has a simple circuit of length k
7. has m simple circuits of length k
8. is connected
9. has an Euler circuit
10. has a Hamiltonian circuit.

Example 10.3.3 **Showing That Two Graphs Are Not Isomorphic**

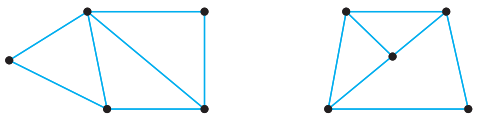
Show that the following pairs of graphs are not isomorphic by finding an isomorphic invariant that they do not share.

a.



G G'

b.



H H'

Solution

a. G has nine edges; G' has only eight.

b. H has a vertex of degree 4; H' does not. ■

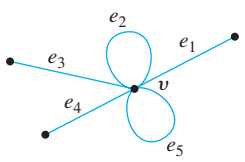
We prove part (3) of Theorem 10.3.2 and leave the proofs of the other parts as exercises.

Example 10.3.4 **Proof of Theorem 10.3.2, Part (3)**

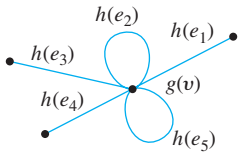
Prove that if G is a graph that has a vertex of degree k and G' is isomorphic to G, then G' has a vertex of degree k.

Proof:

Suppose G and G' are isomorphic graphs and G has a vertex v of degree k, where k is a nonnegative integer. *[We must show that G' has a vertex of degree k.]* Since G and G' are isomorphic, there are one-to-one, onto functions g and h from the vertices of G to the vertices of G' and from the edges of G to the edges of G' that preserve the edge-endpoint functions in the sense that for all edges e and all vertices u of G, u is an endpoint of e if, and only if, $g(u)$ is an endpoint of $h(e)$. An example for a particular vertex v is shown below.



Degree $v = 3 + 2 \cdot 2 = 7$



Degree $g(v) = 3 + 2 \cdot 2 = 7$

Let $e_1, e_2, \ldots, e_m$ be the m distinct edges that are incident on a vertex v in G, where m is a nonnegative integer. Then $h(e_1), h(e_2), \ldots, h(e_m)$ are m distinct edges that are incident on $g(v)$ in G'. *[The reason why $h(e_1), h(e_2), \ldots, h(e_m)$ are distinct is that h is one-to-one and $e_1, e_2, \ldots, e_m$ are distinct. And the reason why $h(e_1), h(e_2), \ldots, h(e_m)$ are incident on $g(v)$ is that g and h preserve the edge-endpoint functions of G and G' and $e_1, e_2, \ldots, e_m$ are incident on v.]*

Also, there are no edges incident on $g(v)$ other than the ones that are images under h of edges incident on v *[because g is onto and g and h preserve the edge-endpoint functions of G and G']*. Thus the number of edges incident on v equals the number of edges incident on $g(v)$.

Finally, an edge e is a loop at v if, and only if, $h(e)$ is a loop at $g(v)$, so the number of loops incident on v equals the number of loops incident on $g(v)$. *[For since g and h preserve the edge-endpoint functions of G and G', a vertex w is an endpoint of e in G if, and only if, $g(w)$ is an endpoint of $h(e)$ in G'. It follows that v is the only endpoint of e in G if, and only if, $g(v)$ is the only endpoint of $h(e)$ in G'.]*

Now the degree of v, which is k, equals the number of edges incident on v that are not loops plus twice the number of edges incident on v that are loops (since each loop contributes 2 to the degree of v). But we have already shown that the number of edges incident on v equals the number of edges incident on $g(v)$, with the number of loops incident on v equal to the number of loops incident on $g(v)$. Hence $g(v)$ also has degree k. ■

Graph Isomorphism for Simple Graphs

When graphs G and G' are both simple, the definition of G being isomorphic to G' can be written without referring to the correspondence between the edges of G and the edges of G'.

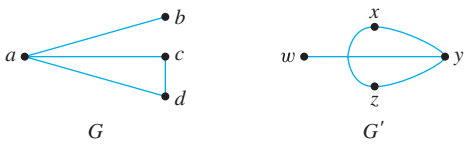
Definition

If G and G' are simple graphs, then **G is isomorphic to G'** if, and only if, there exists a one-to-one correspondence g from the vertex set $V(G)$ of G to the vertex set $V(G')$ of G' that preserves the edge-endpoint functions of G and G' in the sense that for all vertices u and v of G,

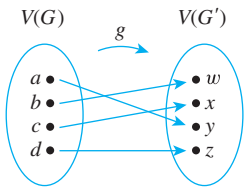
$$\{u, v\} \text{ is an edge in } G \iff \{g(u), g(v)\} \text{ is an edge in } G'. \qquad 10.3.2$$

Example 10.3.5 **Isomorphism of Simple Graphs**

Are the two graphs shown below isomorphic? If so, define an isomorphism.



Solution Yes. Define $g: V(G) \to V(G')$ by the arrow diagram shown below.



Then g is one-to-one and onto by inspection. The fact that g preserves the edge-endpoint functions of G and G' is shown by the following table:

Edges of G	Edges of G'
$\{a, b\}$	$\{y, w\} = \{g(a), g(b)\}$
$\{a, c\}$	$\{y, x\} = \{g(a), g(\mathrm{c})\}$
$\{a, d\}$	$\{y, z\} = \{g(a), g(d)\}$
$\{c, d\}$	$\{x, z\} = \{g(c), g(d)\}$

■

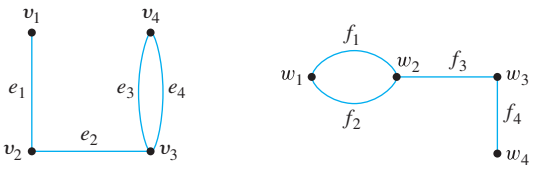
TEST YOURSELF

1. If G and G' are graphs, then G is isomorphic to G' if, and only if, there exist a one-to-one correspondence g from the vertex set of G to the vertex set of G' and a one-to-one correspondence h from the edge set of G to the edge set of G' such that for every vertex v and every edge e in G, v is an endpoint of e if, and only if, _____.
2. A property P is an invariant for graph isomorphism if, and only if, given any graphs G and G', if G has property P and G' is isomorphic to G then _____.
3. Some invariants for graph isomorphisms are _____, _____, _____, _____, _____, _____, _____, _____, _____, and _____.

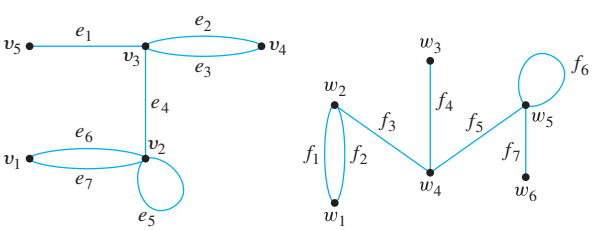
EXERCISE SET 10.3

For each pair of graphs G and G' in 1–5, determine whether G and G' are isomorphic. If they are, give functions g: $V(G) \to V(G')$ and h: $E(G) \to E(G')$ that define the isomorphism. If they are not, give an invariant for graph isomorphism that they do not share.

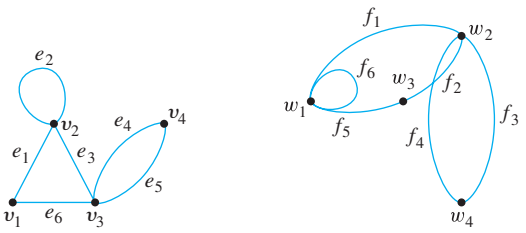
1.



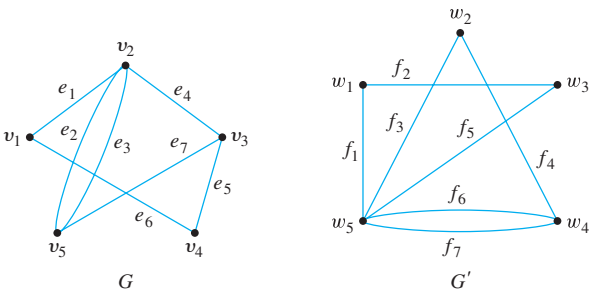
2.



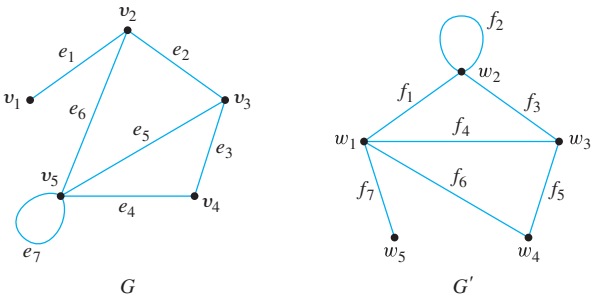
3.



4.

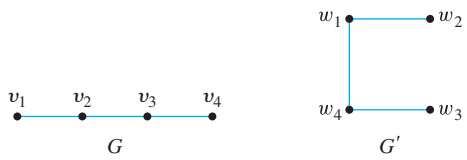


5.

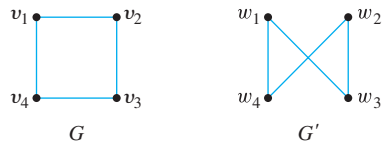


For each pair of simple graphs G and G' in 6–13, determine whether G and G' are isomorphic. If they are, give a function g: $V(G) \to V(G')$ that defines the isomorphism. If they are not, give an invariant for graph isomorphism that they do not share.

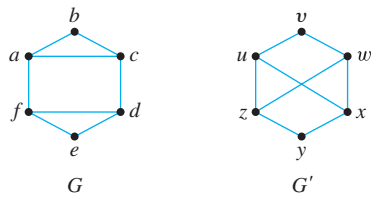
6.



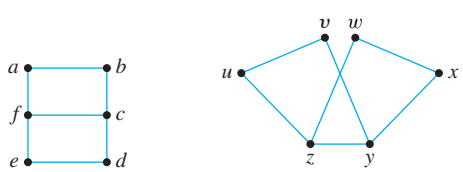
7.



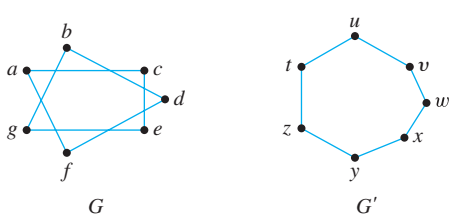
8.



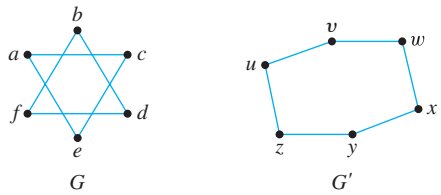
9.



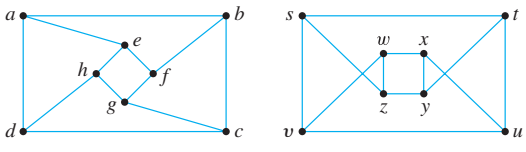
10.



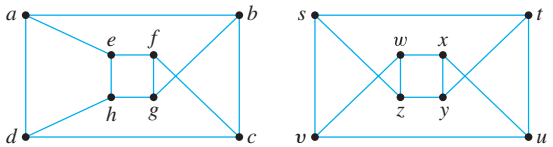
11.



12.



13.



14. Draw all nonisomorphic simple graphs with three vertices.

15. Draw all nonisomorphic simple graphs with four vertices.

16. Draw all nonisomorphic graphs with three vertices and no more than two edges.

17. Draw all nonisomorphic graphs with four vertices and no more than two edges.

***H* 18.** Draw all nonisomorphic graphs with four vertices and three edges.

19. Draw all nonisomorphic graphs with six vertices, all having degree 2.

20. Draw four nonisomorphic graphs with six vertices, two of degree 4 and four of degree 3.

Prove that each of the properties in 21–29 is an invariant for graph isomorphism. Assume that *n*, *m*, and *k* are all nonnegative integers.

21. Has n vertices

22. Has m edges

23. Has a circuit of length k

24. Has a simple circuit of length k

***H* 25.** Has m vertices of degree k

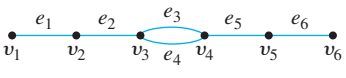
26. Has m simple circuits of length k

***H* 27.** Is connected

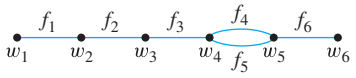
28. Has an Euler circuit

29. Has a Hamiltonian circuit

30. Show that the following two graphs are not isomorphic by supposing they are isomorphic and deriving a contradiction.



G



G'

ANSWERS FOR TEST YOURSELF

1. $g(v)$ is an endpoint of $h(e)$ **2.** G' has property P **3.** has n vertices; has m edges; has a vertex of degree k; has m vertices of degree k; has a circuit of length k; has a simple circuit of length k; has m simple circuits of length k; is connected; has an Euler circuit; has a Hamiltonian circuit

10.4 Trees: Examples and Basic Properties

We are not very pleased when we are forced to accept a mathematical truth by virtue of a complicated chain of formal conclusions and computations, which we traverse blindly, link by link, feeling our way by touch. We want first an overview of the aim and of the road; we want to understand the idea of the proof, the deeper context.
—Hermann Weyl, 1885–1955

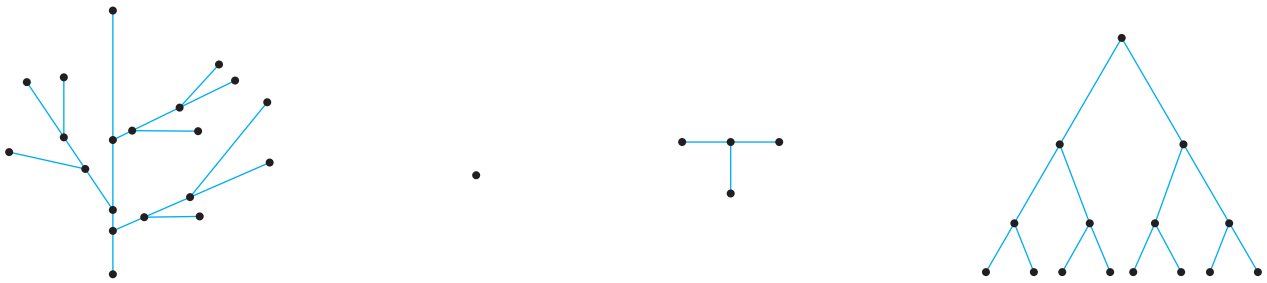
If a friend asks what you are studying and you answer "trees," your friend may think you are taking a course in botany. But trees are also a subject for mathematical investigation. In mathematics, a tree is a connected graph that does not contain any circuits. Mathematical trees are similar in certain ways to their botanical namesakes.

Definition

A graph is said to be **circuit-free** if, and only if, it has no circuits. A graph is called a **tree** if, and only if, it is circuit-free and connected. A **trivial tree** is a graph that consists of a single vertex. A graph is called a **forest** if, and only if, it is circuit-free and not connected.

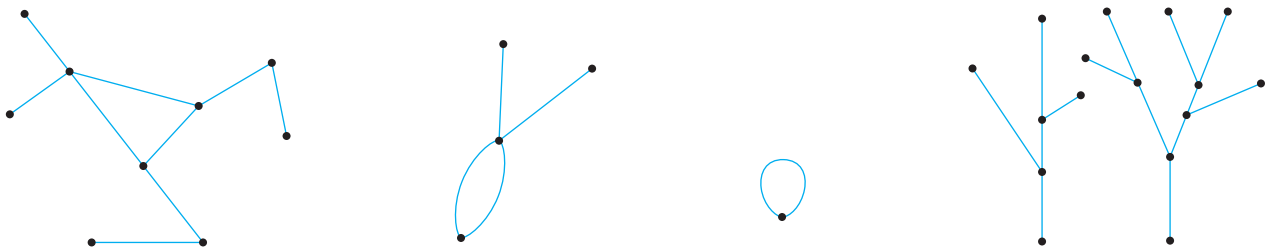
Example 10.4.1 **Trees and Non-trees**

All the graphs shown in Figure 10.4.1 are trees, whereas those in Figure 10.4.2 are not.



(a) (b) (c) (d)

FIGURE 10.4.1 Trees. All the graphs in (a)–(d) are connected and circuit-free.



(a) (b) (c) (d)

FIGURE 10.4.2 Non-trees. The graphs in (a), (b), and (c) all have circuits, and the graph in (d) is not connected. ■

Examples of Trees

The following examples illustrate just a few of the many and varied situations in which mathematical trees arise.

Example 10.4.2 **A Decision Tree**

During orientation week, a college administers a mathematics placement exam to all entering students. The exam consists of two parts, and placement recommendations are made as indicated by the tree shown in Figure 10.4.3. Read the tree from left to right to decide what course should be recommended for a student who scored 9 on part I and 7 on part II.

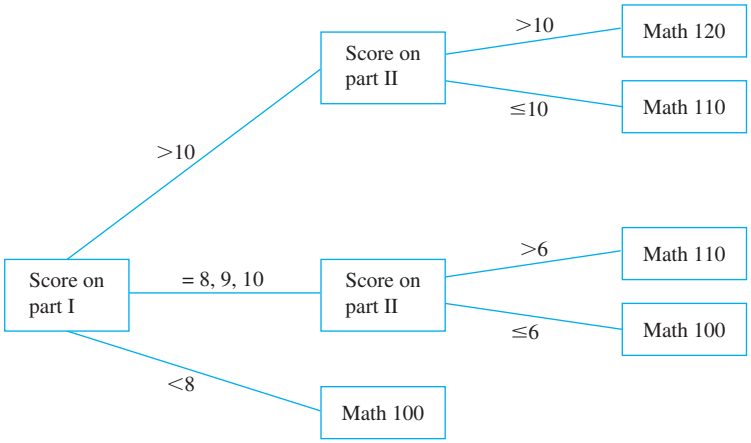


FIGURE 10.4.3

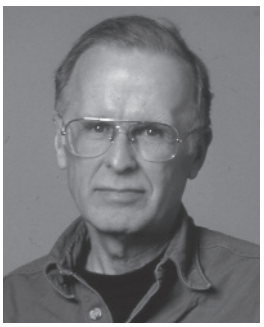
Solution Since the student scored 9 on part I, the score on part II is checked. Since it is greater than 6, the student should be advised to take Math 110. ■

Example 10.4.3 **A Parse Tree**

In the last 30 years, Noam Chomsky and others have developed new ways to describe the syntax (or grammatical structure) of natural languages such as English. As is discussed briefly in Chapter 12, this work has proved useful in constructing compilers for high-level computer languages. In the study of grammars, trees are often used to show the derivation of grammatically correct sentences from certain basic rules. Such trees are called **syntactic derivation trees** or **parse trees**.

A very small subset of English grammar, for example, specifies that

1. a sentence can be produced by writing first a noun phrase and then a verb phrase;
2. a noun phrase can be produced by writing an article and then a noun;
3. a noun phrase can also be produced by writing an article, then an adjective, and then a noun;
4. a verb phrase can be produced by writing a verb and then a noun phrase;
5. one article is "the";
6. one adjective is "young";
7. one verb is "caught";
8. one noun is "man";
9. one (other) noun is "ball."

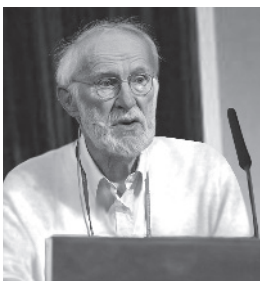


IBM Archives

John Backus
(1924–1998)

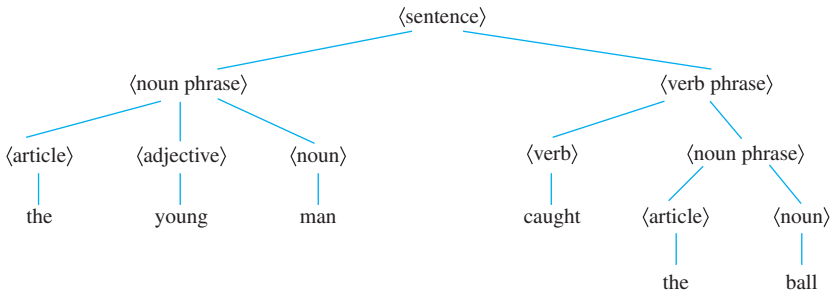
The rules of a grammar are called **productions**. It is customary to express them using the shorthand notation illustrated below. This notation, introduced by John Backus in 1959 and modified by Peter Naur in 1960, was used to describe the computer language Algol and is called the **Backus–Naur notation**. In the notation, the symbol | represents the word *or*, and angle brackets ⟨ ⟩ are used to enclose terms to be defined (such as a sentence or noun phrase).

1. ⟨sentence⟩ ⟶ ⟨noun phrase⟩ ⟨verb phrase⟩
2., 3. ⟨noun phrase⟩ ⟶ ⟨article⟩ ⟨noun⟩ | ⟨article⟩ ⟨adjective⟩ ⟨noun⟩
4. ⟨verb phrase⟩ ⟶ ⟨verb⟩ ⟨noun phrase⟩
5. ⟨article⟩ ⟶ the
6. ⟨adjective⟩ ⟶ young
7. ⟨verb⟩ ⟶ caught
8., 9. ⟨noun⟩ ⟶ man | ball



Peter Naur
(1928–2016)

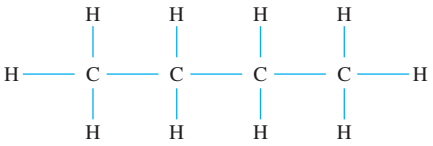
The derivation of the sentence "The young man caught the ball" from the above rules is described by the tree shown below.



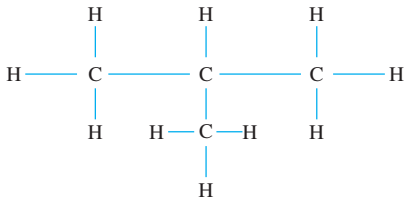
In the study of linguistics, **syntax** refers to the grammatical structure of sentences, and **semantics** refers to the meanings of words and their interrelations. A sentence can be syntactically correct but semantically incorrect, as in the nonsensical sentence "The young ball caught the man," which can be derived from the rules given above. Or a sentence can contain syntactic errors but not semantic ones, as, for instance, when a two-year-old child says, "Me hungry!" ■

Example 10.4.4 **Structure of Hydrocarbon Molecules**

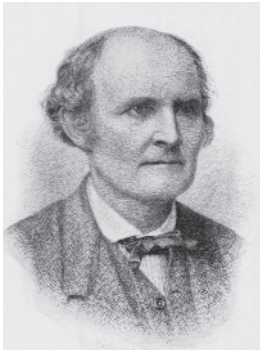
The German physicist Gustav Kirchhoff (1824–1887) was the first to analyze the behavior of mathematical trees in connection with the investigation of electrical circuits. Soon after (and independently), the English mathematician Arthur Cayley used the mathematics of trees to enumerate all isomers for certain hydrocarbons. Hydrocarbon molecules are composed of carbon and hydrogen; each carbon atom can form up to four chemical bonds with other atoms, and each hydrogen atom can form one bond with another atom. Thus the structure of hydrocarbon molecules can be represented by graphs such as those shown below, in which the vertices represent atoms of hydrogen and carbon, denoted H and C, and the edges represent the chemical bonds between them.



Butane



Isobutane



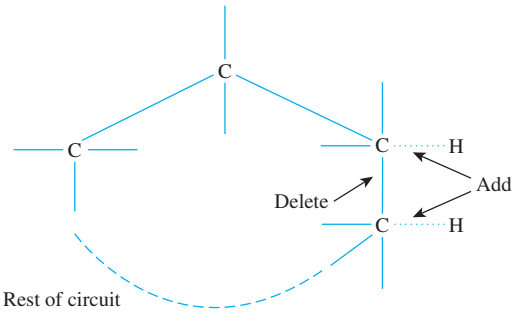
Bettmann/Getty Images

Arthur Cayley (1821–1895)

Note that each of these graphs has four carbon atoms and ten hydrogen atoms, but the two graphs show different configurations of atoms. When two molecules have the same chemical formulas (in this case C_4H_{10}) but different chemical bonds, they are called *isomers.*

Certain *saturated hydrocarbon* molecules contain the maximum number of hydrogen atoms for a given number of carbon atoms. Cayley showed that if such a saturated hydrocarbon molecule has k carbon atoms, then it has $2k + 2$ hydrogen atoms. The first step in doing so is to prove that the graph of such a saturated hydrocarbon molecule is a tree. Prove this using proof by contradiction. (You are asked to finish the derivation of Cayley's result in exercise 4 at the end of this section.)

Solution Suppose there is a hydrocarbon molecule that contains the maximum number of hydrogen atoms for the number of its carbon atoms and whose graph G is not a tree. *[We must derive a contradiction.]* Since G is not a tree, G is not connected or G has a circuit. But the graph of any molecule is connected (all the atoms in a molecule must be connected to each other), and so G must have a nontrivial circuit. Now the edges of the circuit can link only carbon atoms because every vertex of a circuit has degree at least 2 and a hydrogen atom vertex has degree 1. Delete one edge of the circuit and add two new edges to join each of the newly disconnected carbon atom vertices to a hydrogen atom vertex as shown below.



The resulting molecule has two more hydrogen atoms than the given molecule, but the number of carbon atoms is unchanged. This contradicts the supposition that the given molecule has the maximum number of hydrogen atoms for the given number of carbon atoms. Hence the supposition is false, and so G is a tree. ■

Characterizing Trees

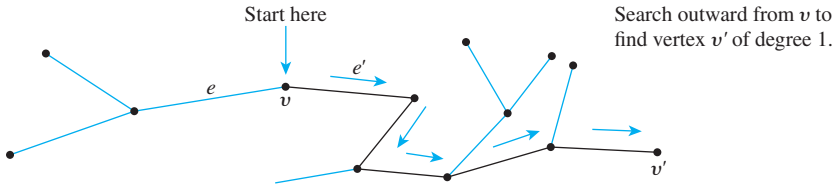
There is a somewhat surprising relation between the number of vertices and the number of edges of a tree. It turns out that if n is a positive integer, then any tree with n vertices (no matter what its shape) has $n - 1$ edges. Perhaps even more surprisingly, a partial converse to this fact is also true—namely, any connected graph with n vertices and $n - 1$ edges is a tree. It follows from these facts that if even one new edge (but no new vertex) is added to a tree, the resulting graph must contain a circuit. Also, from the fact that removing an edge from a circuit does not disconnect a graph, it can be shown that every connected graph has a subgraph that is a tree. It follows that if n is a positive integer, any graph with n vertices and *fewer* than $n - 1$ edges is not connected.

A small but very important fact necessary to derive the first main theorem about trees is that any nontrivial tree must have at least one vertex of degree 1.

Lemma 10.4.1

Any tree that has more than one vertex has at least one vertex of degree 1.

A constructive way to understand this lemma is to imagine being given a tree T with more than one vertex. You pick a vertex v at random and then search outward along a path from v looking for a vertex of degree 1. As you reach each new vertex, you check whether it has degree 1. If it does, you are finished. If it does not, you exit from the vertex along a different edge from the one you entered on. Because T is circuit-free, the vertices included in the path never repeat. And since the number of vertices of T is finite, the process of building a path must eventually terminate. When that happens, the final vertex v' of the path must have degree 1. This process is illustrated below.



This discussion is made precise in the following proof.

Proof:

Let T be a particular but arbitrarily chosen tree that has more than one vertex, and consider the following algorithm:

Step 1: Pick a vertex v of T and let e be an edge incident on v.

[If there were no edge incident on v, then v would be an isolated vertex. But this would contradict the assumption that T is connected (since it is a tree) and has at least two vertices.]

Step 2: While $\deg(v) > 1$, repeat steps 2a, 2b, and 2c:

Step 2a: Choose e' to be an edge incident on v such that $e' \neq e$. *[Such an edge exists because* $\deg(v) > 1$ *and so there are at least two edges incident on* v*.]*

Step 2b: Let v' be the vertex at the other end of e' from v. *[Since T is a tree, e' cannot be a loop and therefore e' has two distinct endpoints.]*

Step 2c: Let $e = e'$ and $v = v'$. *[This is just a renaming process in preparation for repeating step 2.]*

The algorithm just described must eventually terminate because the set of vertices of the tree T is finite and T is circuit-free. When it does, a vertex v of degree 1 will have been found.

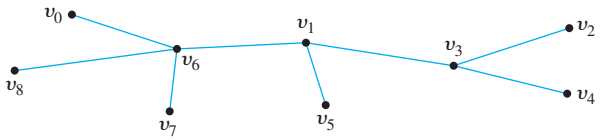
Using Lemma 10.4.1 it is not difficult to show that, in fact, any tree that has more than one vertex has at least *two* vertices of degree 1. This extension of Lemma 10.4.1 is left to exercise 5 at the end of this section. Exercise 29 outlines a nonconstructive proof of this fact that uses proof by contradiction.

Definition

Let T be a tree. If T has at least two vertices, then a vertex of degree 1 in T is called a **leaf** (or a **terminal vertex**), and a vertex of degree greater than 1 in T is called an **internal vertex** (or a **branch vertex**). The unique vertex in a trivial tree is also called a **leaf** or **terminal vertex**.

Example 10.4.5 **Leaves and Internal Vertices in Trees**

Find all leaves (or terminal vertices) and all internal (or branch) vertices in the following tree:



Solution The leaves (or terminal vertices) are v_0, v_2, v_4, v_5, v_7, and v_8. The internal (or branch) vertices are v_6, v_1, and v_3. ■

The following is the first of the two main theorems about trees:

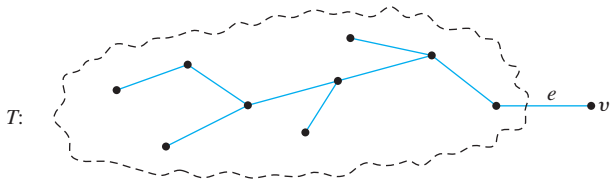
Theorem 10.4.2

For any positive integer n, any tree with n vertices has $n - 1$ edges.

The proof is by mathematical induction. In the inductive step, we assume that any tree with k vertices has $k - 1$ edges, and our job is to show that any tree with $k + 1$ vertices has

k edges. To do this, we start with an arbitrarily chosen tree T with $k+1$ vertices. Then we try to find a vertex and an edge that we can remove from T to create a sub-tree T' with k vertices. If this step is successful, we can apply the inductive hypothesis to show that T' has $k-1$ edges, and when we replace the vertex and edge that we removed, we can conclude that T has k edges.

In order to find the vertex and edge to remove from T, we use Lemma 10.4.1, which states that T has a vertex v of degree 1. Since T is connected, v is attached to the rest of T by a single edge e as sketched below.



If e and v are removed from T, what remains is a tree T' with $(k+1)-1=k$ vertices. By inductive hypothesis, then, T' has $k-1$ edges. Now the original tree T has one more vertex and one more edge than T'. Hence T must have $(k-1)+1=k$ edges. A formal version of this argument is given below.

Proof (by mathematical induction):

Let the property $P(n)$ be the sentence

Any tree with n vertices has $n-1$ edges. ←$P(n)$

We use mathematical induction to show that this property is true for every integer $n \geq 1$.

Show that P(1) is true: Let T be any tree with one vertex. Then T has zero edges (since it contains no loops). Since $0 = 1-1$, then $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k+1) is true:

Suppose k is any positive integer for which $P(k)$ is true. In other words, suppose that

Any tree with k vertices has $k-1$ edges. ← $P(k)$ inductive hypothesis

We must show that $P(k+1)$ is true. In other words, we must show that

Any tree with $k+1$ vertices has $(k+1)-1=k$ edges. ←$P(k+1)$

Note We can't assume anything about T except that it has $k+1$ vertices.

Let T be a particular but arbitrarily chosen tree with $k+1$ vertices. *[We must show that T has k edges.]* Since k is a positive integer, $(k+1) \geq 2$, and so T has more than one vertex. Hence by Lemma 10.4.1, T has a vertex v of degree 1. Also, since T has more than one vertex, there is at least one other vertex in T besides v. Thus there is an edge e connecting v to the rest of T. Define a subgraph T' of T so that

$$V(T') = V(T) - \{v\} \quad \text{and} \quad E(T') = E(T) - \{e\}.$$

Then

1. The number of vertices of T' is $(k+1)-1=k$.
2. T' is circuit-free (since T is circuit-free, and removing an edge and a vertex cannot create a circuit).
3. T' is connected (see exercise 24 at the end of this section).

Hence, by the definition of tree, T' is a tree. Since T' has k vertices, by inductive hypothesis

$$\begin{aligned}\text{the number of edges of } T' &= (\text{the number of vertices of } T')-1\\ &= k-1.\end{aligned}$$

It follows that

$$\begin{aligned}\text{the number of edges of } T &= (\text{the number of edges of } T')+1\\ &= (k-1)+1\\ &= k.\end{aligned}$$

[This is what was to be shown.]

Example 10.4.6 **Determining Whether a Graph Is a Tree**

A graph G has ten vertices and twelve edges. Is it a tree?

Solution No. By Theorem 10.4.2, any tree with ten vertices has nine edges, not twelve. ■

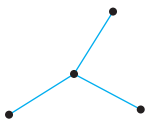
Example 10.4.7 **Finding Trees Satisfying Given Conditions**

Find all nonisomorphic trees with four vertices.

Solution By Theorem 10.4.2, any tree with four vertices has three edges. Thus the total degree of a tree with four vertices must be 6. Also, every tree with more than one vertex has at least two vertices of degree 1 (see the comment following Lemma 10.4.1 and exercises 5 and 29 at the end of this section). Thus the following combinations of degrees for the vertices are the only ones possible:

$$1, 1, 1, 3 \quad \text{and} \quad 1, 1, 2, 2.$$

There are two nonisomorphic trees corresponding to both of these possibilities, as shown below.



and

■

To prove the second major theorem about trees, we need another lemma.

Lemma 10.4.3

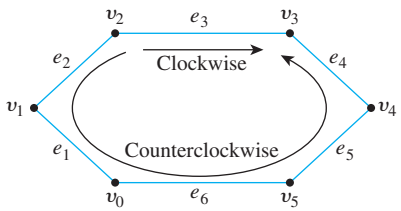
If G is any connected graph, C is any circuit in G, and any one of the edges of C is removed from G, then the graph that remains is connected.

Essentially, the reason why Lemma 10.4.3 is true is that any two vertices in a circuit are connected by two distinct paths. It is possible to draw the graph so that one of these goes "clockwise" and the other goes "counterclockwise" around the circuit. For example, in the circuit below, the clockwise path from v_2 to v_3 is

$$v_2 e_3 v_3$$

and the counterclockwise path from v_2 to v_3 is

$$v_2 e_2 v_1 e_1 v_0 e_6 v_5 e_5 v_4 e_4 v_3, \quad \text{where } v_6 = v_0.$$



Proof:

Suppose G is a connected graph, C is a circuit in G, and e is an edge of C. Form a subgraph G' of G by removing e from G. Thus

$$V(G') = V(G)$$
$$E(G') = E(G) - \{e\}.$$

We must show that G' is connected. *[To show a graph is connected, we must show that if u and w are any vertices of the graph, then there exists a walk in G' from u to w.]* Suppose u and w are any two vertices of G'. *[We must find a walk from u to w.]* Since the vertex sets of G and G' are the same, because u and w are both vertices of G, and since G is connected, there is a walk W in G from u to w.

Case 1 (e is not an edge of W): The only edge in G that is not in G' is e, so in this case W is also a walk in G'. Hence u is connected to w by a walk in G'.

Case 2 (e is an edge of W): In this case the walk W from u to w includes a section of the circuit C that contains e. Let C be denoted as follows:

$$C\colon v_0 e_1 v_1 e_2 v_2 \cdots e_n v_n \,(= v_0).$$

Now e is one of the edges of C, so, to be specific, let $e = e_k$. Then the walk W contains either the sequence

$$v_{k-1} e_k v_k \quad \text{or} \quad v_k e_k v_{k-1}.$$

If W contains $v_{k-1} e_k v_k$, connect v_{k-1} to v_k by taking the "counterclockwise" walk W' defined as follows:

$$W'\colon v_{k-1} e_{k-1} v_{k-2} \cdots v_0 e_n v_{n-1} \cdots e_{k+1} v_k \quad \text{where } v_n = v_0.$$

An example showing how to go from u to w while avoiding e_k is given in Figure 10.4.4.

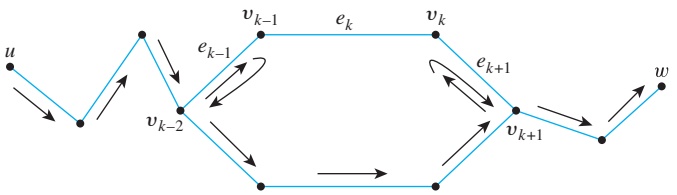


FIGURE 10.4.4 An Example of a Walk from u to w That Does Not Include Edge e_k

If W contains $v_k e_k v_{k-1}$, connect v_k to v_{k-1} by taking the "clockwise" walk W'' defined as follows:

$$W'': v_k e_{k+1} v_{k+1} \cdots v_n e_1 v_1 e_2 \cdots e_{k-1} v_{k-1} \quad \text{where } v_n = v_0.$$

Now patch either W' or W'' into W to form a new walk from u to w. For instance, to patch W' into W, start with the section of W from u to v_{k-1}, then take W' from v_{k-1} to v_k, and finally take the section of W from v_k to w. If this new walk still contains an occurrence of e, just repeat the process described previously until all occurrences are eliminated. *[This must happen eventually since the number of occurrences of e in C is finite.]* The result is a walk from u to w that does not contain e and hence is a walk in G'.

The previous arguments show that both in case 1 and in case 2 there is a walk in G' from u to w. Since the choice of u and w was arbitrary, G' is connected.

The second major theorem about trees is a modified converse for Theorem 10.4.2.

Theorem 10.4.4

For any positive integer n, if G is a connected graph with n vertices and $n - 1$ edges, then G is a tree.

Proof:

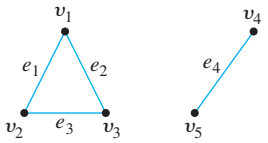
Let n be a positive integer and suppose G is a particular but arbitrarily chosen graph that is connected and has n vertices and $n - 1$ edges. *[We must show that G is a tree. Now a tree is a connected, circuit-free graph. Since we already know G is connected, it suffices to show that G is circuit-free.]* Suppose G is not circuit-free. That is, suppose G has a circuit C. *[We must derive a contradiction.]* By Lemma 10.4.3, an edge of C can be removed from G to obtain a graph G' that is connected. If G' has a circuit, then repeat this process: Remove an edge of the circuit from G' to form a new connected graph. Continue repeating the process of removing edges from circuits until eventually a graph G'' is obtained that is connected and is circuit-free. By definition, G'' is a tree. Since no vertices were removed from G to form G'', G'' has n vertices just as G does. Thus, by Theorem 10.4.2, G'' has $n - 1$ edges. But the supposition that G has a circuit implies that at least one edge of G is removed to form G''. Hence G'' has no more than $(n - 1) - 1 = n - 2$ edges, which contradicts its having $n - 1$ edges. So the supposition is false. Hence G is circuit-free, and therefore G is a tree *[as was to be shown]*.

Theorem 10.4.4 is not a full converse of Theorem 10.4.2. Although it is true that every *connected* graph with n vertices and $n - 1$ edges (where n is a positive integer) is a tree, it is not true that *every* graph with n vertices and $n - 1$ edges is a tree.

Example 10.4.8 **A Graph with n Vertices and $n - 1$ Edges That Is Not a Tree**

Give an example of a graph with five vertices and four edges that is not a tree.

Solution By Theorem 10.4.4, such a graph cannot be connected. One example of such an unconnected graph is shown below.



■

Corollary 10.4.5

If G is any graph with n vertices and m edges, where m and n are positive integers and $m \geq n$, then G has a circuit.

Proof (by contradiction):
Suppose not. That is, suppose there is a graph G with n vertices and m edges, where m and n are positive integers and $m \geq n$, and suppose G does not have a circuit. Let $G_1, G_2, \ldots, G_k$ be the connected components of G, and let $n_1, n_2, \ldots, n_k$ be the number of vertices of $G_1, G_2, \ldots, G_k$, respectively. Because $G_1, G_2, \ldots, G_k$ are the connected components of G,

$$\sum_{i=1}^{k} n_i = n.$$

Since G does not have a circuit, none of $G_1, G_2, \ldots, G_k$ have circuits either. So, since each is connected, each is a tree. By Theorem 10.4.4, the number of edges of each G_i is n_{i-1}. Now because G is composed of its connected components,

$$\begin{aligned}
\text{the number of edges of } G &= \sum_{i=1}^{k} (\text{the number of edges of } G_i) \\
&= (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) \\
&= (n_1 + n_2 + \cdots + n_k) - \underbrace{(1 + 1 + \cdots + 1)}_{k \text{ 1's}} \\
&= n - k, \\
&< n \qquad \text{since } k \geq 1.
\end{aligned}$$

Thus the number of edges of G is less than n, which contradicts the hypothesis that the number of edges of G, namely, m, is greater than or equal to n. Hence the supposition is false and G has a circuit.

TEST YOURSELF

1. A circuit-free graph is a graph with _____.
2. A forest is a graph that is _____, and a tree is a graph that is _____.
3. A trivial tree is a graph that consists of _____.
4. Any tree with at least two vertices has at least one vertex of degree _____.
5. If a tree T has at least two vertices, then a terminal vertex (or leaf) in T is a vertex of degree _____ and an internal vertex (or branch vertex) in T is a vertex of degree _____.
6. For any positive integer n, any tree with n vertices has _____.
7. For any positive integer n, if G is a connected graph with n vertices and $n - 1$ edges then _____.

EXERCISE SET 10.4

1. Read the tree in Example 10.4.2 from left to right to answer the following questions.
   a. A student scored 12 on part I and 4 on part II. What course should the student take?
   b. A student scored 8 on part I and 9 on part II. What course should the student take?
2. Draw trees to show the derivations of the following sentences from the rules given in Example 10.4.3.
   a. The young ball caught the man.
   b. The man caught the young ball.

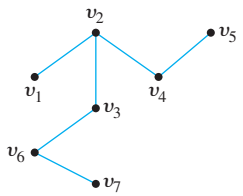
H 3. What is the total degree of a tree with n vertices? Why?

4. Let G be the graph of a hydrocarbon molecule with the maximum number of hydrogen atoms for the number of its carbon atoms.
   a. Draw the graph of G if G has three carbon atoms and eight hydrogen atoms.
   b. Draw the graphs of three isomers of C_5H_{12}.
   c. Use Example 10.4.4 and exercise 3 to prove that if the vertices of G consist of k carbon atoms and m hydrogen atoms, then G has a total degree of $2k + 2m - 2$.
   H d. Prove that if the vertices of G consist of k carbon atoms and m hydrogen atoms, then G has a total degree of $4k + m$.
   e. Equate the results of (c) and (d) to prove Cayley's result that a saturated hydrocarbon molecule with k carbon atoms and a maximum number of hydrogen atoms has $2k + 2$ hydrogen atoms.

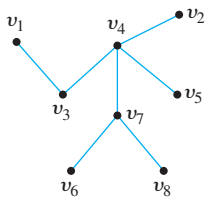
H 5. Extend the argument given in the proof of Lemma 10.4.1 to show that a tree with more than one vertex has at least two vertices of degree 1.

6. If graphs are allowed to have an infinite number of vertices and edges, then Lemma 10.4.1 is false. Give a counterexample that shows this. In other words, give an example of an "infinite tree" (a connected, circuit-free graph with an infinite number of vertices and edges) that has no vertex of degree 1.
7. Find all leaves (or terminal vertices) and all internal (or branch) vertices for the following trees.

a.



b.



In each of 8–21, either draw a graph with the given specifications or explain why no such graph exists.

8. Tree, nine vertices, nine edges
9. Graph, connected, nine vertices, nine edges
10. Graph, circuit-free, nine vertices, six edges
11. Tree, six vertices, total degree 14
12. Tree, five vertices, total degree 8
13. Graph, connected, six vertices, five edges, has a circuit

14. Graph, two vertices, one edge, not a tree

15. Graph, circuit-free, seven vertices, four edges

16. Tree, twelve vertices, fifteen edges

17. Graph, six vertices, five edges, not a tree

18. Tree, five vertices, total degree 10

19. Graph, connected, ten vertices, nine edges, has a circuit

20. Simple graph, connected, six vertices, six edges

21. Tree, ten vertices, total degree 24

22. A connected graph has twelve vertices and eleven edges. Does it have a vertex of degree 1? Why?

23. A connected graph has nine vertices and twelve edges. Does it have a circuit? Why?

24. Suppose that v is a vertex of degree 1 in a connected graph G and that e is the edge incident on v. Let G' be the subgraph of G obtained by removing v and e from G. Must G' be connected? Why?

25. A graph has eight vertices and six edges. Is it connected? Why?

***H* 26.** If a graph has n vertices and $n - 2$ or fewer edges, can it be connected? Why?

27. A circuit-free graph has ten vertices and nine edges. Is it connected? Why?

***H* 28.** Is a circuit-free graph with n vertices and at least $n - 1$ edges connected? Why?

29. Prove that every nontrivial tree has at least two vertices of degree 1 by filling in the details and completing the following argument: Let T be a nontrivial tree and let S be the set of all paths from one vertex to another in T. Among all the paths in S, choose a path P with a maximum number of edges. (Why is it possible to find such a P?) What can you say about the initial and final vertices of P? Why?

30. Find all nonisomorphic trees with five vertices.

31. a. Prove that the following is an invariant for graph isomorphism: A vertex of degree i is adjacent to a vertex of degree j.

***H* b.** Find all nonisomorphic trees with six vertices.

ANSWERS FOR TEST YOURSELF

1. no circuits **2.** circuit-free and not connected; connected and circuit-free **3.** a single vertex (and no edges) **4.** 1 **5.** 1; greater than 1 (*Or:* at least 2) **6.** $n - 1$ edges **7.** G is a tree

10.5 Rooted Trees

Let us grant that the pursuit of mathematics is a divine madness of the human spirit, a refuge from the goading urgency of contingent happenings.
—Alfred North Whitehead, 1861–1947

An outdoor tree is rooted and so is the kind of family tree that shows all the descendants of one particular person. The terminology and notation of rooted trees blends the language of botanical trees and that of family trees. In mathematics, a rooted tree is a tree in which one vertex has been distinguished from the others and is designated the *root*. Given any other vertex v in the tree, there is a unique path from the root to v. (After all, if there were two distinct paths, a circuit could be constructed.) The number of edges in such a path is called the level of v, and the *height* of the tree is the length of the longest such path. It is traditional in drawing rooted trees to place the root at the top (as is done in family trees) and show the branches descending from it.

Definition

A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the **root**. The **level** of a vertex is the number of edges along the unique path between it and the root. The **height** of a rooted tree is the maximum level of any vertex of the tree. Given the root or any internal vertex v of a rooted tree, the **children** of v are all those vertices that are adjacent to v and are one level farther away from the root than v. If w is a child of v, then v is called the **parent** of w, and two distinct vertices that are both children of the same parent are called **siblings**. Given two distinct vertices v and w, if v lies on the unique path between w and the root, then v is an **ancestor** of w and w is a **descendant** of v.

These terms are illustrated in Figure 10.5.1.

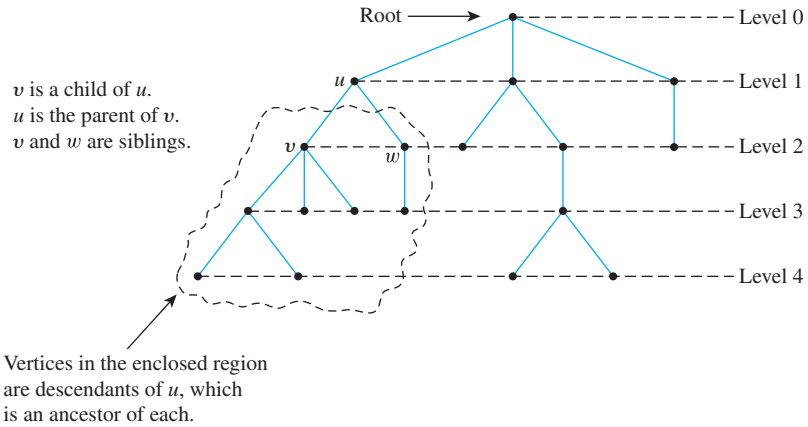
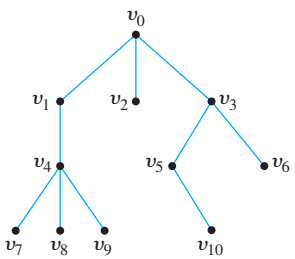


FIGURE 10.5.1 A Rooted Tree

Example 10.5.1 **Rooted Trees**

Consider the tree with root v_0 shown below.

a. What is the level of v_5?
b. What is the level of v_0?
c. What is the height of this rooted tree?
d. What are the children of v_3?
e. What is the parent of v_2?
f. What are the siblings of v_8?
g. What are the descendants of v_3?
h. How many leaves (terminal vertices) are on the tree?



Solution

a. 2 b. 0 c. 3 d. v_5 and v_6 e. v_0 f. v_7 and v_9 g. v_5, v_6, v_{10} h. 6

Note that in the tree shown below, the root is v_0, v_1 has level 1, v_1 is the child of v_0, and both v_0 and v_1 are leaves (terminal vertices).

Binary Trees

When every vertex in a rooted tree has at most two children and each child is designated either the (unique) left child or the (unique) right child, the result is a *binary tree.*

Definition

A **binary tree** is a rooted tree in which every parent has at most two children. Each child in a binary tree is designated either a **left child** or a **right child** (but not both), and every parent has at most one left child and one right child. A **full binary tree** is a binary tree in which each parent has exactly two children.

Given any parent v in a binary tree T, if v has a left child, then the **left subtree** of v is the binary tree whose root is the left child of v, whose vertices consist of the left child of v and all its descendants, and whose edges consist of all those edges of T that connect the vertices of the left subtree. The **right subtree** of v is defined analogously.

These terms are illustrated in Figure 10.5.2.

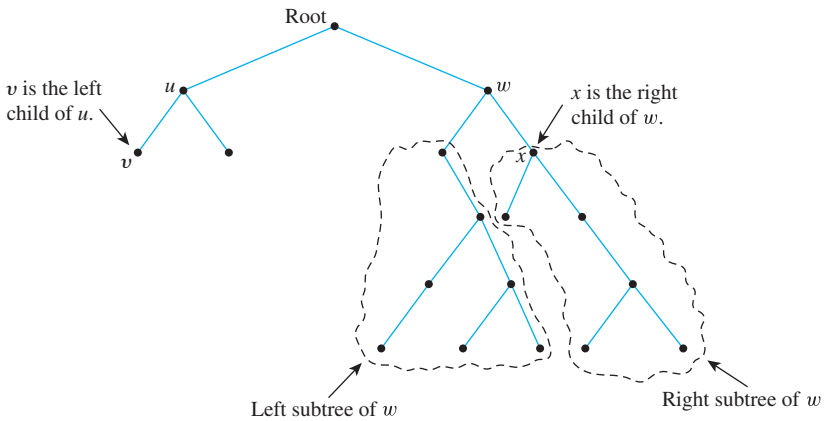
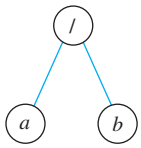


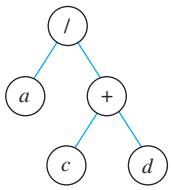
FIGURE 10.5.2 A Binary Tree

Example 10.5.2 **Representation of Algebraic Expressions**

Binary trees are used in many ways in computer science. One use is to represent algebraic expressions with arbitrary nesting of balanced parentheses. For instance, the following (labeled) binary tree represents the expression a/b: The operator is at the root and acts on the left and right children of the root in left-to-right order.

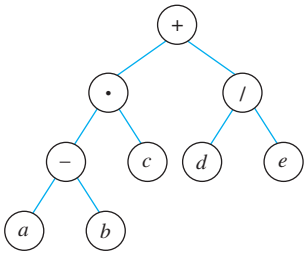


More generally, the binary tree shown below represents the expression $a/(c+d)$. In such a representation, the internal vertices are arithmetic operators, the leaves are variables, and the operator at each vertex acts on its left and right subtrees in left-to-right order.



Draw a binary tree to represent the expression $((a-b)\cdot c)+(d/e)$.

Solution



■

An interesting theorem about binary trees says that if you know the number of internal vertices of a full binary tree, then you can calculate both the total number of vertices and the number of leaves, and conversely. More specifically, a full binary tree with k internal vertices has a total of $2k+1$ vertices of which $k+1$ are leaves.

Theorem 10.5.1

If k is a positive integer and T is a full binary tree with k internal vertices, then (1) T has a total of $2k+1$ vertices, and (2) T has $k+1$ leaves.

Proof:

Suppose k is a positive integer and T is a full binary tree with k internal vertices. (1) Observe that the set of all vertices of T can be partitioned into two disjoint subsets: the set of all vertices that have a parent and the set of all vertices that do not have a parent. Now there is just one vertex that does not have a parent, namely the root. Also, since every internal vertex of a full binary tree has exactly two children, the number of vertices that have a parent is twice the number of parents, or $2k$, since each parent is an internal vertex. Hence

$$\begin{bmatrix}\text{the total number}\\ \text{of vertices of } T\end{bmatrix} = \begin{bmatrix}\text{the number of}\\ \text{vertices that}\\ \text{have a parent}\end{bmatrix} + \begin{bmatrix}\text{the number of}\\ \text{vertices that do}\\ \text{not have a parent}\end{bmatrix}$$
$$= \quad 2k \quad + \quad 1.$$

(continued on page 736)

(2) Because it is also true that the total number of vertices of T equals the number of internal vertices plus the number of leaves,

$$\begin{bmatrix}\text{the total number}\\ \text{of vertices of } T\end{bmatrix} = \begin{bmatrix}\text{the number of}\\ \text{internal vertices}\end{bmatrix} + \begin{bmatrix}\text{the number of}\\ \text{leaves}\end{bmatrix}$$

$$= \quad k \quad + \begin{bmatrix}\text{the number of}\\ \text{leaves}\end{bmatrix}.$$

Now equate the two expressions for the total number of vertices of T:

$$2k + 1 = k + \begin{bmatrix}\text{the number of}\\ \text{leaves}\end{bmatrix}.$$

Solving this equation gives

$$\begin{bmatrix}\text{the number of}\\ \text{leaves}\end{bmatrix} = (2k + 1) - k = k + 1.$$

Thus the total number of vertices is $2k + 1$ and the number of leaves is $k + 1$ *[as was to be shown]*.

Example 10.5.3 **Determining Whether a Certain Full Binary Tree Exists**

Is there a full binary tree that has 10 internal vertices and 13 terminal vertices?

Solution No. By Theorem 10.5.1, a full binary tree with 10 internal vertices has $10 + 1 = 11$ leaves, not 13. ■

Another interesting theorem about binary trees specifies the maximum number of leaves of a binary tree of a given height. Specifically, the maximum number of leaves of a binary tree of height h is 2^h. Another way to say this is that a binary tree with t leaves has height of at least $\log_2 t$.

Theorem 10.5.2

For every integer $h \geq 0$, if T is any binary tree with height h and t leaves, then

$$t \leq 2^h.$$

Equivalently: $\log_2 t \leq h$.

Proof (by strong mathematical induction):

Let $P(h)$ be the sentence

If T is any binary tree of height h, then T has at most 2^h leaves. ← $P(h)$

Show that P(0) is true: We must show that if T is any binary tree of height 0, then T has at most 2^0 leaves. Suppose T is a tree of height 0. Then T consists of a single vertex, the root. By definition this is also a leaf, and so the number of leaves is $t = 1 = 2^0 = 2^h$. Hence $t \leq 2^h$ *[as was to be shown]*.

Show that for every integer $k \geq 0$, if $P(i)$ is true for each integer i from 0 through k, then it is true for $k+1$:
Let k be any integer with $k \geq 0$, and suppose that

> For each integer i from 0 through k, if T is any binary tree of height i, then T has at most 2^i leaves. ← inductive hypothesis

We must show that

> If T is any binary tree of height $k+1$, then T has at most 2^{k+1} leaves. ← $P(k+1)$

Let T be a binary tree of height $k+1$, root v, and t leaves. Because $k \geq 0$, we have that $k+1 \geq 1$ and so v has at least one child.

Case 1 (v has only one child): In this case, we may assume without loss of generality that v's child is a left child v_L, and that v_L is the root of the subtree T_L of v. (This situation is illustrated in Figure 10.5.3.) Let t_L be the number of leaves in T_L. By inductive hypothesis, $t_L \leq 2^k$ because the height of T_L is one less than the height of T, which is $k+1$. Also since the root v has only one child, v is also a leaf, and hence the total number of leaves in T is one more than the number of leaves in T_L. Finally, $2^k \geq 2^0 = 1$ because $k \geq 0$.

Therefore,

$$t = t_L + 1 \leq 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{(k+1)}.$$

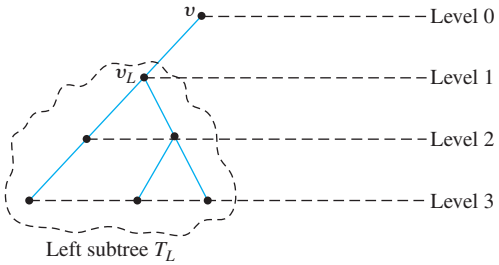


FIGURE 10.5.3 A Binary Tree Whose Root Has One Child

Case 2 (v has two children): In this case, v has both a left child, v_L, and a right child, v_R, and v_L and v_R are roots of a left subtree T_L and a right subtree T_R. Note that T_L and T_R are binary trees because T is a binary tree. (This situation is illustrated in Figure 10.5.4.)

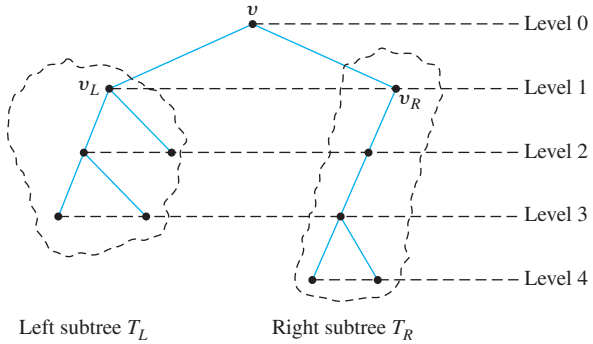


FIGURE 10.5.4 A Binary Tree Whose Root Has Two Children

(continued on page 738)

Let t_L and t_R be the numbers of leaves in T_L and T_R, respectively, and let h_L and h_R be the heights of T_L and T_R, respectively. Because T has height $k+1$, then $h_L \leq k$ and $h_R \leq k$, and so, by inductive hypothesis,

$$t_L \leq 2^{h_L} \quad \text{and} \quad t_R \leq 2^{h_R}.$$

Now the leaves of T consist exactly of the leaves of T_L together with the leaves of T_R. Therefore,

$$t = t_L + t_R \leq 2^{h_L} + 2^{h_R} \qquad \text{by inductive hypothesis since } h_L \leq k \text{ and } h_R \leq k.$$

Hence,

$$t \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} \qquad \text{by basic algebra.}$$

Thus the number of leaves is at most 2^{k+1} *[as was to be shown].*

Since both the basis step and the inductive step have been proved, we conclude that for every integer $h \geq 0$, if T is any binary tree with height h and t leaves, then $t \leq 2^h$.

The equivalent inequality $\log_2 t \leq h$ follows from the fact that the logarithmic function with base 2 is increasing. In other words, for all positive real numbers x and y,

$$\text{if } x < y \text{ then } \log_2 x < \log_2 y.$$

Thus if we apply the logarithmic function with base 2 to both sides of

$$t \leq 2^h,$$

we obtain

$$\log_2 t \leq \log_2(2^h).$$

Now by definition of logarithm, $\log_2(2^h) = h$ *[because* $\log_2(2^h)$ *is the exponent to which* 2 *must be raised to obtain* 2^h*]*. Hence

$$\log_2 t \leq h$$

[as was to be shown].

Example 10.5.4 **Determining Whether a Certain Binary Tree Exists**

Is there a binary tree that has height 5 and 38 leaves?

Solution No. By Theorem 10.5.2, any binary tree T with height 5 has at most $2^5 = 32$ leaves, so such a tree cannot have 38 leaves. ■

Corollary 10.5.3

A full binary tree of height h has 2^h leaves.

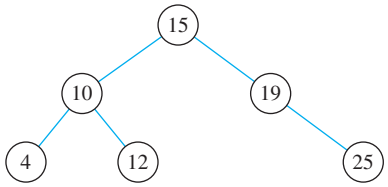
To prove the corollary, start with the proof of Theorem 10.5.2, change the words "binary tree" to "full binary tree," change the words "at most" to "exactly," and change the

$\leq$ sign to the $=$ sign. Also delete Case 1 because the root of a full binary tree of height at least 1 is guaranteed to have two children.

Binary Search Trees

A binary search tree is a kind of binary tree in which data records, such as customer information, can be stored, searched, and processed very efficiently. To place records into a binary search tree, it must be possible to arrange them in a total order. In case they do not have a natural total order of their own, an element of a totally ordered set, such as a number or a word and called a **key**, may be added to each record. The keys are inserted into the vertices of the tree and provide access to the records to which they are attached.

Once it is built, a binary search tree has the following property: **for every internal vertex *v*, all the keys in the left subtree of *v* are less than the key in *v*, and all the keys in the right subtree of *v* are greater than the key in *v***. For example, check that the following is a binary search tree for the set of records with the following keys: 15, 10, 19, 25, 12, 4.



To build a binary search tree, start by making a root and insert a key into it. To add a new key, compare it to the key at the root. If the new key is less than the key at the root, give the root a left child and insert the new key into it. If the key is greater than the key at the root, give the root a right child and insert the new key into it. After the first couple of keys have been added, the root and other vertices may already have left and right children. So to add a key at a subsequent stage, work down the tree to find a place to put the new key, starting at the root and either moving left or right depending on whether the new key is less or greater than the key at the vertex to which it is currently being compared. This outline is expressed more precisely in the following algorithm.

Algorithm 10.5.1 Building a Binary Search Tree

Input: A totally ordered, nonempty set K of keys

Algorithm Body:
Initialize T to have one vertex, the root, and no edges. Choose a key from K to insert into the root.

while (there are still keys to be added)
Choose a key, *newkey*, from K to add. Let the root be called v, let $key(v)$ be the key at the root, and let $success = 0$.
while ($success = 0$)
if ($newkey < key(v)$)
then if (v has a left child), call the left child v_L and let $v := v_L$
else do 1. add a vertex v_L to T as the left child for v
2. add an edge to T to join v to v_L
3. insert *newkey* as the key for v_L
4. let $success := 1$ **end do**

(continued on page 740)

if ($newkey > key(v)$)
then if v has a right child
then call the right child v_R, and let $v := v_R$
else do 1. add a vertex v_R to T as the right child for v
2. add an edge to T to join v to v_R
3. insert $newkey$ as the key for v_R
4. let $success := 1$ **end do**
end while
end while
Output: A binary search tree T for the set K of keys

Example 10.5.5 **Steps for Building a Binary Search Tree**

Go through the steps to build a binary search tree for the keys 15, 10, 19, 25, 12, 4, and insert the keys in the order in which they are listed. For simplicity, use the same names for the vertices and their associated keys.

Solution

Insert 15: Make 15 the root.

Insert 10: Compare 10 to 15.
Since $10 < 15$ and 15 does not have a left child, make 10 the left child of 15 and add an edge joining 15 and 10.

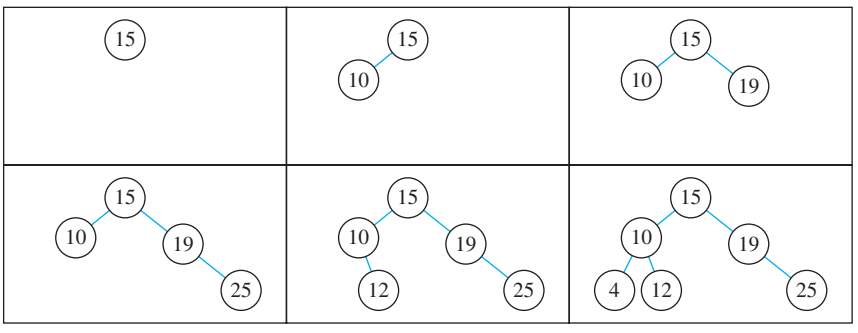
Insert 19: Compare 19 to 15.
Since $19 > 15$ and 15 does not have a right child, make 19 the right child of 15 and add an edge joining 15 and 19.

Insert 25: Compare 25 to 15.
Since $25 > 15$ and 15 has a right child, namely 19, compare 25 to 19.
Since $25 > 19$ and 19 does not have a right child, make 25 the right child of 19 and add an edge joining 19 and 25.

Insert 12: Compare 12 to 15.
Since $12 < 15$ and 15 has a left child, namely 10, compare 12 to 10.
Since $12 > 10$ and 10 does not have a right child, make 12 the right child of 10 and add an edge joining 10 and 12.

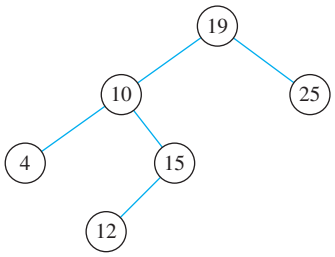
Insert 4: Compare 4 to 15.
Since $4 < 15$ and 15 has a left child, namely 10, compare 4 to 10.
Since $4 < 10$ and 10 does not have a left child, make 4 the left child of 10 and add an edge joining 10 and 4.

The sequence of steps is shown in the following diagrams.



■

Note that the algorithm does not specify an order in which keys are to be added as the tree is being built. In fact, adding keys in a different order usually results in a different binary search tree for the given set of keys. For example, if the keys shown in Example 10.5.5 are added in the order 19, 10, 25, 4, 15, 12, the result is the following binary search tree:

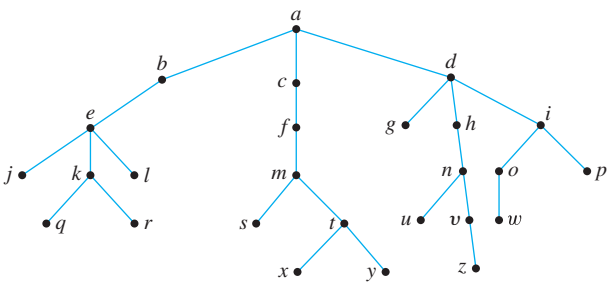


TEST YOURSELF

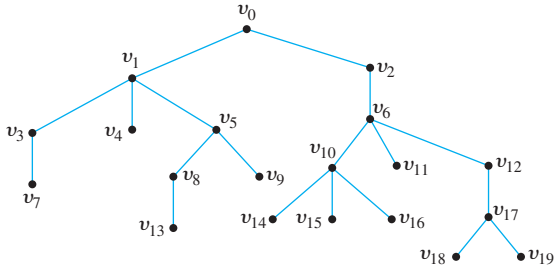
1. A rooted tree is a tree in which _____. The level of a vertex in a rooted tree is _____. The height of a rooted tree is _____.
2. A binary tree is a rooted tree in which _____.
3. A full binary tree is a rooted tree in which _____.
4. If k is a positive integer and T is a full binary tree with k internal vertices, then T has a total of _____ vertices and has _____ leaves.
5. If T is a binary tree that has t leaves and height h, then t and h are related by the inequality _____.

EXERCISE SET 10.5

1. Consider the tree shown below with root a.
   a. What is the level of n?
   b. What is the level of a?
   c. What is the height of this rooted tree?
   d. What are the children of n?
   e. What is the parent of g?
   f. What are the siblings of j?
   g. What are the descendants of f?
   h. How many leaves (terminal vertices) are on the tree?



2. Consider the tree shown below with root v_0.
   a. What is the level of v_8?
   b. What is the level of v_0?
   c. What is the height of this rooted tree?
   d. What are the children of v_{10}?
   e. What is the parent of v_5?
   f. What are the siblings of v_1?
   g. What are the descendants of v_{12}?
   h. How many leaves (terminal vertices) are on the tree?



3. Draw binary trees to represent the following expressions:

a. $a \cdot b - (c/(d+e))$ **b.** $a/(b - c \cdot d)$

In each of 4–20, either draw a graph with the given specifications or explain why no such graph exists.

4. Full binary tree, five internal vertices

5. Full binary tree, five internal vertices, seven leaves

6. Full binary tree, seven vertices, of which four are internal vertices

7. Full binary tree, twelve vertices

8. Full binary tree, nine vertices

9. Binary tree, height 3, seven leaves

10. Full binary tree, height 3, six leaves

11. Binary tree, height 3, nine leaves

12. Full binary tree, eight internal vertices, seven leaves

13. Binary tree, height 4, eight leaves

14. Full binary tree, seven vertices

15. Full binary tree, nine vertices, five internal vertices

16. Full binary tree, four internal vertices

17. Binary tree, height 4, eighteen leaves

18. Full binary tree, sixteen vertices

19. Full binary tree, height 3, seven leaves

20. What can you deduce about the height of a binary tree if you know that it has the following properties?
a. Twenty-five leaves
b. Forty leaves
c. Sixty leaves

In 21–25, use the steps of Algorithm 10.5.1 to build binary search trees. Use numerical order in 21 and alphabetical order in 22–25. In parts (a) and (b) of 21 and 22, the elements in the lists are the same, but the trees are different because the lists are ordered differently.

21. **a.** 16, 24, 21, 3, 18, 9, 7
b. 16, 7, 3, 21, 18, 24, 9

22. **a.** Asia, Africa, Australia, Antarctica, Europe, North America, South America
b. Australia, Antarctica, Africa, North America, Asia, South America, Europe

23. Carpe diem. Seize the day. Make your lives extraordinary.[1]

24. May the force be with you.[2]

25. All good things which exist are the fruits of originality.[3]

ANSWERS FOR TEST YOURSELF

1. one vertex is distinguished from the others and is called the root; the number of edges along the unique path between it and the root; the maximum level of any vertex of the tree **2.** every parent has at most two children **3.** every parent has exactly two children **4.** $2k + 1$; $k + 1$ **5.** $t \leq 2^h$, or, equivalently, $\log_2 t \leq h$

10.6 Spanning Trees and a Shortest Path Algorithm

I contend that each science is a real science insofar as it is mathematics.
—Immanuel Kant, 1724–1804

An airline company wants to expand service to the midwestern part of the United States and has received permission from the U.S. Federal Aviation Authority to fly any of the routes shown in Figure 10.6.1.

[1] adapted from *Dead Poets Society* (film)
[2] *Star Wars* (film)
[3] John Stuart Mill, *On Liberty*

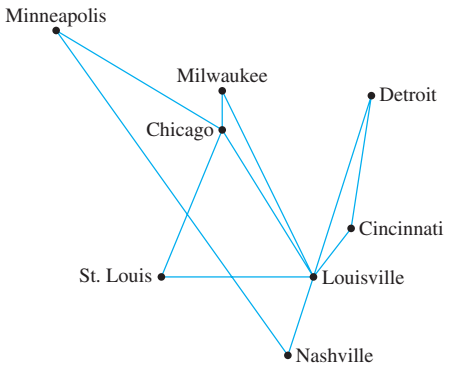


FIGURE 10.6.1

The company wishes to legitimately advertise service to all the cities shown but, for reasons of economy, wants to use the least possible number of individual routes to connect them. One possible route system is given in Figure 10.6.2.

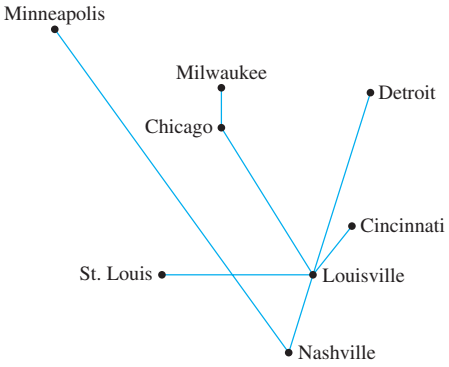


FIGURE 10.6.2

Clearly this system joins all the cities. Is the number of individual routes minimal? The answer is yes, and the reason may surprise you.

The fact is that the graph of any system of routes that satisfies the company's wishes is a tree, because if the graph were to contain a circuit, then one of the routes in the circuit could be removed without disconnecting the graph (by Lemma 10.4.3), and that would give a smaller total number of routes. Now any tree with eight vertices has seven edges. Therefore, any system of routes that connects all eight vertices and yet minimizes the total number of routes consists of seven routes.

Definition

A **spanning tree** for a graph G is a subgraph of G that contains every vertex of G and is a tree.

The preceding discussion contains the essence of the proof of the following proposition:

Proposition 10.6.1

1. Every connected graph has a spanning tree.
2. Any two spanning trees for a graph have the same number of edges.

(continued on page 744)

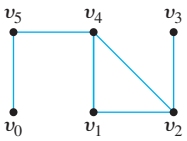
Proof of part (1) of Proposition 10.6.1:

Suppose G is a connected graph. If G is circuit-free, then G is its own spanning tree and we are done. If not, then G has at least one circuit C_1. By Lemma 10.4.3, the subgraph of G obtained by removing an edge from C_1 is connected. If this subgraph is circuit-free, then it is a spanning tree and we are done. If not, then it has at least one circuit C_2, and, as above, an edge can be removed from C_2 to obtain a connected subgraph. Continuing in this way, we can remove successive edges from circuits, until eventually we obtain a connected, circuit-free subgraph T of G. *[This must happen at some point because the number of edges of G is finite, and at no stage does removal of an edge disconnect the subgraph.]* Also, T contains every vertex of G because no vertices of G were removed in constructing it. Thus T is a spanning tree for G.

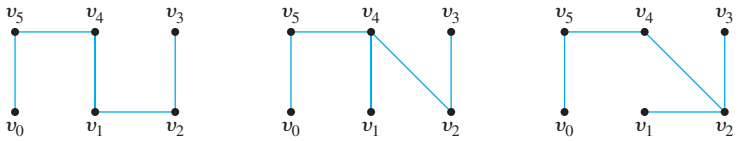
You are asked to prove part (2) of Proposition 10.6.1 in exercise 17 at the end of this section.

Example 10.6.1 **Spanning Trees**

Find all spanning trees for the graph G pictured below.



Solution The graph G has one circuit $v_2v_1v_4v_2$, and removing any edge of the circuit gives a tree. Thus, as shown below, there are three spanning trees for G.



Minimum Spanning Trees

The graph of the routes allowed by the U.S. Federal Aviation Authority shown in Figure 10.6.1 can be annotated by adding the distances (in miles) between each pair of cities. This is done in Figure 10.6.3.

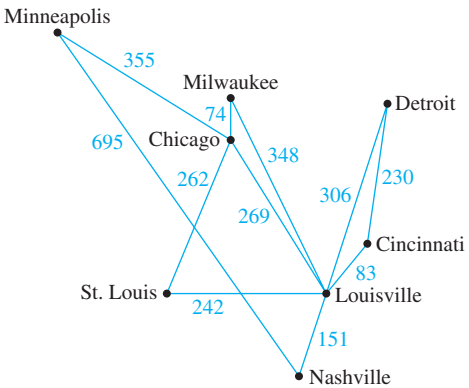


FIGURE 10.6.3

Now suppose the airline company wants to serve all the cities shown, but with a route system that minimizes the total mileage of the system as a whole. Note that such a system is a tree, because if the system contained a circuit, removal of an edge from the circuit would not affect a person's ability to reach every city in the system from every other (again, by Lemma 10.4.3), but it would reduce the total mileage of the system.

More generally, a graph whose edges are labeled with numbers (known as *weights*) is called a *weighted graph*. A *minimum-weight spanning tree*, or simply a *minimum spanning tree*, is a spanning tree for which the sum of the weights of all the edges is as small as possible.

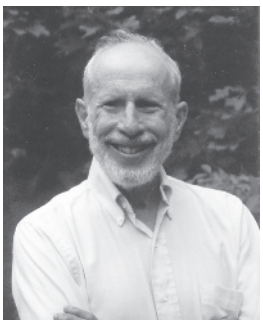
Definition and Notation

A **weighted graph** is a graph for which each edge has an associated positive real number **weight**. The sum of the weights of all the edges is the **total weight** of the graph. A **minimum spanning tree** for a connected, weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph.

If G is a weighed graph and e is an edge of G, then $\boldsymbol{w(e)}$ denotes the weight of e and $\boldsymbol{w(G)}$ denotes the total weight of G.

The problem of finding a minimum spanning tree for a graph is certainly solvable. One solution is to list all spanning trees for the graph, compute the total weight of each, and choose one for which this total is a minimum. (The well-ordering principle for the integers guarantees the existence of such a minimum total.) This solution, however, is inefficient in its use of computing time because the number of distinct spanning trees is so large. For instance, a complete graph with n vertices has n^{n-2} spanning trees. Even using the fastest computers available today, examining all such trees in a graph with approximately 100 vertices would require more time than is estimated to remain in the life of the universe.

In 1956 and 1957 Joseph B. Kruskal and Robert C. Prim each described much more efficient algorithms to construct minimum spanning trees. Even for large graphs, both algorithms can be implemented so as to take relatively short computing times.



Courtesy of Joyce Kruskal

Joseph Kruskal (1928–2010)

Kruskal's Algorithm

In Kruskal's algorithm, the edges of a connected, weighted graph are examined one by one in order of increasing weight. At each stage the edge being examined is added to what will become the minimum spanning tree, provided that this addition does not create a circuit. After $n - 1$ edges have been added (where n is the number of vertices of the graph), these edges, together with the vertices of the graph, form a minimum spanning tree for the graph.

Algorithm 10.6.1 Kruskal

Input: *G [a connected, weighted graph with n vertices, where n is a positive integer]*

Algorithm Body:

[Build a subgraph T of G to consist of all the vertices of G with edges added in order of increasing weight. At each stage, let m be the number of edges of T.]

1. Initialize T to have all the vertices of G and no edges.
2. Let E be the set of all the edges of G, and let $m := 0$.

(continued on page 746)

3. **while** $(m < n - 1)$

3a. Find an edge e in E of least weight.

3b. Delete e from E.

3c. **if** addition of e to the edge set of T does not produce a circuit **then** add e to the edge set of T and set $m := m + 1$

end while

Output: *T [T is a minimum spanning tree for G.]*

The following example shows how Kruskal's algorithm works for the graph of the airline route system.

Example 10.6.2 **Action of Kruskal's Algorithm**

Describe the action of Kruskal's algorithm on the graph shown in Figure 10.6.4, where $n = 8$.

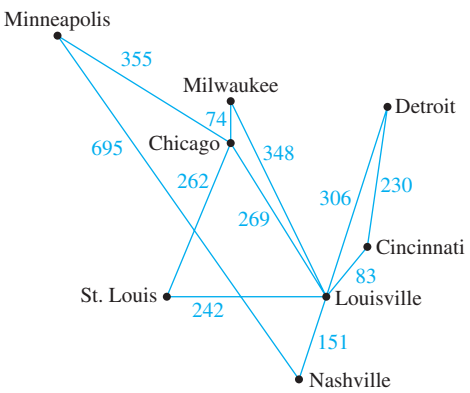


FIGURE 10.6.4

Solution

Iteration Number	Edge Considered	Weight	Action Taken
1	Chicago–Milwaukee	74	added
2	Louisville–Cincinnati	83	added
3	Louisville–Nashville	151	added
4	Cincinnati–Detroit	230	added
5	St. Louis–Louisville	242	added
6	St. Louis–Chicago	262	added
7	Chicago–Louisville	269	not added
8	Louisville–Detroit	306	not added
9	Louisville–Milwaukee	348	not added
10	Minneapolis–Chicago	355	added

The tree produced by Kruskal's algorithm is shown in Figure 10.6.5.

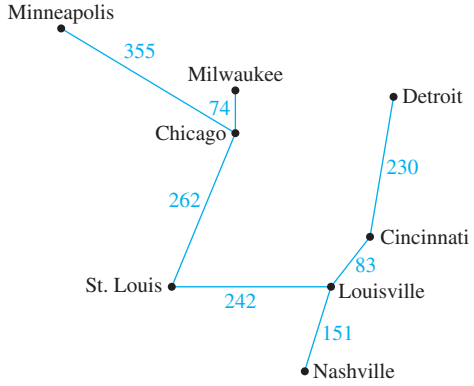


FIGURE 10.6.5

When Kruskal's algorithm is used on a graph in which some edges have the same weight as others, more than one minimum spanning tree can occur as output. To make the output unique, the edges of the graph can be placed in an array and edges having the same weight can be added in the order they appear in the array.

It is not obvious from the description of Kruskal's algorithm that it does what it is supposed to do. To be specific, what guarantees that it is possible at each stage to find an edge of least weight whose addition does not produce a circuit? And if such edges can be found, what guarantees that they will all eventually connect? And if they do connect, what guarantees that the resulting tree has minimum weight? Of course, the mere fact that Kruskal's algorithm is printed in this book may lead you to believe that everything works out. But the questions above are real, and they deserve serious answers.

Theorem 10.6.2 Correctness of Kruskal's Algorithm

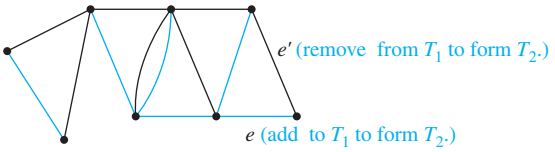
When a connected, weighted graph is input to Kruskal's algorithm, the output is a minimum spanning tree.

Proof: Suppose that G is a connected, weighted graph with n vertices and that T is a subgraph of G produced when G is input to Kruskal's algorithm. Clearly T is circuit-free *[since no edge that completes a circuit is ever added to T].* Also, T is connected. For as long as T has more than one connected component, the set of edges of G that can be added to T without creating a circuit is nonempty. *[The reason is that since G is connected, given any vertex v_1 in one connected component C_1 of T and any vertex v_2 in another connected component C_2, there is a path in G from v_1 to v_2. Since C_1 and C_2 are distinct, there is an edge e of this path that is not in T. Adding e to T does not create a circuit in T, because deletion of an edge from a circuit does not disconnect a graph and deletion of e would.]* The preceding arguments show that T is circuit-free and connected. Since by construction T contains every vertex of G, T is a spanning tree for G.

Next we show that T has minimum weight. Let T_1 be any minimum spanning tree for G such that the number of edges T_1 and T have in common is a maximum. Suppose that $T \neq T_1$. Then there is an edge e in T that is not an edge of T_1. *[Since trees T and T_1 both have the same vertex set, if they differ at all, they must have different, but*

(continued on page 748)

same-size, edge sets.] Now adding e to T_1 produces a graph with a unique circuit (see exercise 19 at the end of this section). Let e' be an edge of this circuit such that e' is not in T. *[Such an edge must exist because T is a tree and hence circuit-free.]* Let T_2 be the graph obtained from T_1 by removing e' and adding e. This situation is illustrated below.



The entire graph is G. T_1 has black edges. e is in T but not T_1. e' is in T_1 but not T.

Note that T_2 has $n - 1$ edges and n vertices and that T_2 is connected *[since by Lemma 10.4.3 the subgraph obtained by removing an edge from a circuit in a connected graph is connected]*. Consequently, T_2 is a spanning tree for G. In addition,

$$w(T_2) = w(T_1) - w(e') + w(e).$$

Now $w(e) \leq w(e')$ because at the stage in Kruskal's algorithm when e was added to T, e' was available to be added *[since it was not already in T, and at that stage its addition could not produce a circuit since e was not in T]*, and e' would have been added had its weight been less than that of e. Thus

$$\begin{aligned} w(T_2) &= w(T_1) - \underbrace{[w(e') - w(e)]}_{\geq 0} \\ &\leq w(T_1). \end{aligned}$$

But T_1 is a minimum spanning tree. So since T_2 is a spanning tree with weight less than or equal to the weight of T_1, T_2 is also a minimum spanning tree for G.

Finally, note that by construction, T_2 has one more edge in common with T than T_1 does, which contradicts the choice of T_1 as a minimum spanning tree for G with a maximum number of edges in common with T. Thus the supposition that $T \neq T_1$ is false, and hence T itself is a minimum spanning tree for G.

Nokia Bell Labs

Robert Prim (born 1921)

Prim's Algorithm

Prim's algorithm works differently from Kruskal's. It builds a minimum spanning tree T by expanding outward in connected links from some vertex. One edge and one vertex are added at each stage. The edge added is the one of least weight that connects the vertices already in T with those not in T, and the vertex is the endpoint of this edge that is not already in T.

Algorithm 10.6.2

Input: *G [a connected, weighted graph with n vertices where n is a positive integer]*

Algorithm Body:

[Build a subgraph T of G by starting with any vertex v of G and attaching edges (with their endpoints) one by one to an as-yet-unconnected vertex of G, each time choosing an edge of least weight that is adjacent to a vertex of T.]

1. Pick a vertex v of G and let T be the graph with one vertex, v, and no edges.
2. Let V be the set of all vertices of G except v.
3. **for** $i := 1$ **to** $n - 1$
   - 3a. Find an edge e of G such that (1) e connects T to one of the vertices in V, and (2) e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e that is in V.
   - 3b. Add e and w to the edge and vertex sets of T, and delete w from V.

   next i

Output: *T [T is a minimum spanning tree for G.]*

The following example shows how Prim's algorithm works for the graph of the airline route system.

Example 10.6.3 **Action of Prim's Algorithm**

Describe the action of Prim's algorithm for the graph in Figure 10.6.6 using the Minneapolis vertex as a starting point.

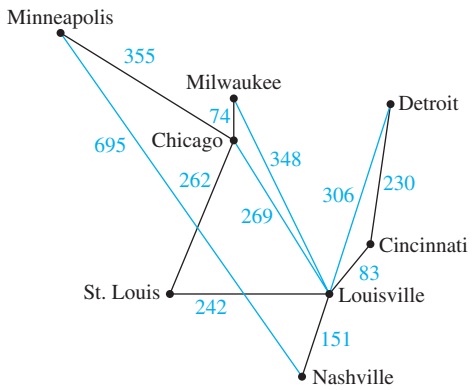


FIGURE 10.6.6

Solution

Iteration Number	Vertex Added	Edge Added	Weight
0	Minneapolis		
1	Chicago	Minneapolis–Chicago	355
2	Milwaukee	Chicago–Milwaukee	74
3	St. Louis	Chicago–St. Louis	262
4	Louisville	St. Louis–Louisville	242
5	Cincinnati	Louisville–Cincinnati	83
6	Nashville	Louisville–Nashville	151
7	Detroit	Cincinnati–Detroit	230

■

Note that the tree obtained is the same as that obtained by Kruskal's algorithm, but the edges are added in a different order.

As with Kruskal's algorithm, in order to ensure a unique output, the edges of the graph could be placed in an array and those with the same weight could be added in the order they appear in the array. It is not hard to see that when a connected graph is input to Prim's algorithm, the result is a spanning tree. What is not so clear is that this spanning tree is a minimum. The proof of the following theorem establishes that it is.

Theorem 10.6.3 Correctness of Prim's Algorithm

When a connected, weighted graph G is input to Prim's algorithm, the output is a minimum spanning tree for G.

Proof:

Let G be a connected, weighted graph, and suppose G is input to Prim's algorithm. At each stage of execution of the algorithm, an edge must be found that connects a vertex in a subgraph to a vertex outside the subgraph. As long as there are vertices outside the subgraph, the connectedness of G ensures that such an edge can always be found. *[For if one vertex in the subgraph and one vertex outside it are chosen, then by the connectedness of G there is a walk in G linking the two. As one travels along this walk, at some point one moves along an edge from a vertex inside the subgraph to a vertex outside the subgraph.]*

Now it is clear that the output T of Prim's algorithm is a tree because the edge and vertex added to T at each stage are connected to other edges and vertices of T and because at no stage is a circuit created since each edge added connects vertices in two disconnected sets. *[Consequently, removal of a newly added edge produces a disconnected graph, whereas by Lemma 10.4.3, removal of an edge from a circuit produces a connected graph.]* Also, T includes every vertex of G because T, being a tree with $n - 1$ edges, has n vertices *[and that is all G has]*. Thus T is a spanning tree for G.

Next we show that T has minimum weight. Suppose there is a minimum spanning tree for G, T_1, such that the number of edges T_1 and T have in common is a maximum, but $T \neq T_1$. Then there is an edge e in T that is not an edge of T_1. *[Since trees T and T_1 both have the same vertex set if they differ at all, they must have different, same-size edge sets.]* Of all such edges, let e be the last that was added when T was constructed using Prim's algorithm. Let S be the set of vertices of T just before the addition of e. Then one endpoint, say v of e, is in S and the other, say w, is not. Since T_1 is a spanning tree, there is a path in T_1 joining v to w. And since $v \in S$ and $w \notin S$, as one travels along this path, one must encounter an edge e' that joins a vertex in S to one that is not in S and that therefore is not in T because e was the last edge added to T. Now at the stage when e was added to T, e' could have been added and it *would* have been added instead of e had its weight been less than that of e. Since e' was not added at that stage, we conclude that

$$w(e') \geq w(e).$$

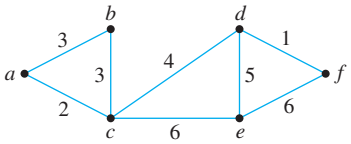
Let T_2 be the graph obtained from T_1 by removing e' and adding e. *[Thus T_2 has one more edge in common with T than T_1 does.]* Note that T_2 is a tree. The reason is that since e' is part of a path in T_1 from v to w, and e connects v and w, adding e to T_1 creates a circuit. When e' is removed from this circuit, the resulting subgraph remains connected and has the same number of edges as T. In fact, T_2 is a spanning tree for G since no vertices were removed in forming T_2 from T_1. The argument showing that $w(T_2) \leq w(T_1)$ is left as an exercise. *[It is virtually identical*

to part of the proof of Theorem 10.6.2.] It follows that T_2 is a minimum spanning tree for G.

By construction, T_2 has one more edge in common with T than T_1 does, which contradicts the choice of T_1 as a minimum spanning tree for G, not equal to T, with a maximum number of edges in common with T. It follows that $T = T_1$, and hence T itself is a minimum spanning tree for G.

Example 10.6.4 **Finding Minimum Spanning Trees**

Find all minimum spanning trees for the following graph. Use Kruskal's algorithm and Prim's algorithm starting at vertex a. Indicate the order in which edges are added to form each tree.



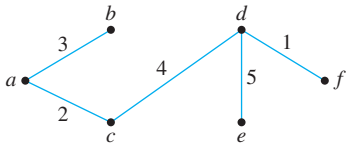
Solution When Kruskal's algorithm is applied, edges are added in one of the following two orders:

1. $\{d, f\}$, $\{a, c\}$, $\{a, b\}$, $\{c, d\}$, $\{d, e\}$
2. $\{d, f\}$, $\{a, c\}$, $\{b, c\}$, $\{c, d\}$, $\{d, e\}$

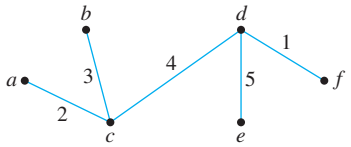
When Prim's algorithm is applied starting at a, edges are added in one of the following two orders:

1. $\{a, c\}$, $\{a, b\}$, $\{c, d\}$, $\{d, f\}$, $\{d, e\}$
2. $\{a, c\}$, $\{b, c\}$, $\{c, d\}$, $\{d, f\}$, $\{d, e\}$

Thus, as shown below, there are two distinct minimum spanning trees for this graph.



(a)



(b)

Dijkstra's Shortest Path Algorithm

Although the trees produced by Kruskal's and Prim's algorithms have the least possible total weight compared to all other spanning trees for the given graph, they do not always reveal the shortest distance between any two points on the graph. For instance, according to the complete route system shown in Figure 10.6.3, one can fly directly from Nashville to Minneapolis for a distance of 695 miles, whereas if you use the minimum spanning tree shown in Figure 10.6.5 the only way to fly from Nashville to Minneapolis is by going through Louisville, St. Louis, and Chicago, which gives a total distance of $151 + 242 + 262 + 355 = 1{,}010$ miles and the unpleasantness of three changes of plane.

In 1959 the computing pioneer, Edsger Dijkstra (see Section 5.5), developed an algorithm to find the shortest path between a starting vertex and an ending vertex in a weighted graph in which all the weights are positive. It is somewhat similar to Prim's algorithm in that it works outward from a starting vertex a, adding vertices and edges one by one to construct a tree T. However, it differs from Prim's algorithm in the way it chooses the next vertex to add, ensuring that for each added vertex v, the length of the shortest path from a to v has been identified.

At the start of execution of the algorithm, each vertex u of G is given a label $L(u)$, which indicates the current best estimate of the length of the shortest path from a to u. $L(a)$ is initially set equal to 0 because the shortest path from a to a has length 0, but, because there is no previous information about the lengths of the shortest paths from a to any other vertices of G, the label $L(u)$ of each vertex u other than a is initially set equal to a number, denoted ∞, that is greater than the sum of the weights of all the edges of G. As execution of the algorithm progresses, the values of $L(u)$ are changed, eventually becoming the actual lengths of the shortest paths from a to u in G.

Because T is built up outward from a, at each stage of execution of the algorithm the only vertices that are candidates to join T are those that are adjacent to at least one vertex of T. Thus at each stage of Dijkstra's algorithm, the graph G can be thought of as divided into three parts: the tree T that is being built up, the set of "fringe" vertices that are adjacent to at least one vertex of the tree, and the rest of the vertices of G. Each fringe vertex is a candidate to be the next vertex added to T. The one that is chosen is the one for which the length of the shortest path to it from a through T is a minimum among all the vertices in the fringe.

An essential observation underlying Dijkstra's algorithm is that after each addition of a vertex v to T, the only fringe vertices for which a shorter path from a might be found are those that are adjacent to v *[because the length of the path from a to v was a minimum among all the paths from a to vertices in what was then the fringe]*. So after each addition of a vertex v to T, each fringe vertex u adjacent to v is examined and two numbers are compared: the current value of $L(u)$ and the value of $L(v) + w(v, u)$, where $L(v)$ is the length of the shortest path to v (in T) and $w(v, u)$ is the weight of the edge joining v and u. If $L(v) + w(v, u) < L(u)$, then the value of $L(u)$ is changed to $L(v) + w(v, u)$.

At the beginning of execution of the algorithm, the tree consists only of the vertex a, and $L(a) = 0$. When execution terminates, $L(z)$ is the length of a shortest path from a to z.

As with Kruskal's and Prim's algorithms for finding minimum spanning trees, there is a simple but dramatically inefficient way to find the shortest path from a to z: compute the lengths of all the paths and choose one that is shortest. The problem is that even for relatively small graphs, using this method to find a shortest path could require billions of years, whereas Dijkstra's algorithm could do the job in a few seconds.

Algorithm 10.6.3 Dijkstra

Input: *G [a connected simple graph with a positive weight for every edge], ∞ [a number greater than the sum of the weights of all the edges in the graph], $w(u, v)$ [the weight of edge $\{u, v\}$], a [the starting vertex], z [the ending vertex]*

Algorithm Body:

1. Initialize T to be the graph with vertex a and no edges. Let $V(T)$ be the set of vertices of T, and let $E(T)$ be the set of edges of T.
2. Let $L(a) = 0$, and for all vertices in G except a, let $L(u) = \infty$.
   [The number $L(x)$ is called the label of x.]
3. Initialize v to equal a and F to be $\{a\}$.
   [The symbol v is used to denote the vertex most recently added to T.]
4. **while** $(z \notin V(T))$
   - **4a.** $F := (F - \{v\}) \cup \{\text{vertices that are adjacent to } v \text{ and are not in } V(T)\}$
     [The set F is called the fringe. Each time a vertex is added to T, it is removed from the fringe and the vertices adjacent to it are added to the fringe if they are not already in the fringe or the tree T.]
   - **4b.** For each vertex u that is adjacent to v and is not in $V(T)$,
     if $L(v) + w(v, u) < L(u)$ **then**

     $$L(u) := L(v) + w(v, u)$$
     $$D(u) := v$$

     [Note that adding v to T does not affect the labels of any vertices in the fringe F except those adjacent to v. Also, when $L(u)$ is changed to a smaller value, the notation $D(u)$ is introduced to keep track of which vertex in T gave rise to the smaller value.]
   - **4c.** Find a vertex x in F with the smallest label
     Add vertex x to $V(T)$, and add edge $\{D(x), x\}$ to $E(T)$
     $v := x$ *[This statement sets up the notation for the next iteration of the loop.]*

   end while

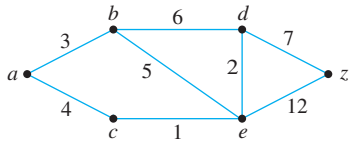
Output: $L(z)$ *[$L(z)$, a nonnegative integer, is the length of the shortest path from a to z.]*

Note The unique path in the tree T from a to z is the shortest path in G from a to z.

The action of Dijkstra's algorithm is illustrated by the flow of the drawings in Example 10.6.5.

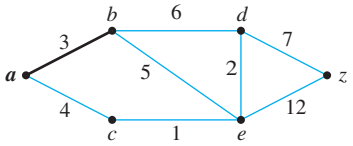
Example 10.6.5 **Action of Dijkstra's Algorithm**

Show the steps in the execution of Dijkstra's shortest path algorithm for the graph shown below with starting vertex a and ending vertex z.



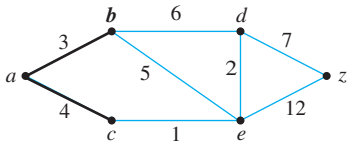
Solution

Step 1: Going into the **while** loop: $V(T) = \{a\}$, $E(T) = \varnothing$, and $F = \{a\}$



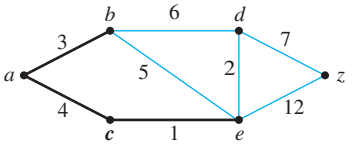
During iteration:
$F = \{b, c\}$, $L(b) = 3$, $L(c) = 4$.
Since $L(b) < L(c)$, b is added to $V(T)$, $D(b) = a$, and $\{a, b\}$ is added to $E(T)$.

Step 2: Going into the **while** loop: $V(T) = \{a, b\}$, $E(T) = \{\{a, b\}\}$



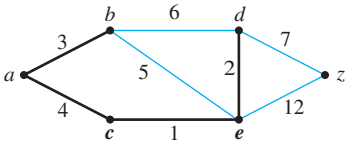
During iteration:
$F = \{c, d, e\}$, $L(c) = 4$, $L(d) = 9$, $L(e) = 8$.
Since $L(c) < L(d)$ and $L(c) < L(e)$, c is added to $V(T)$, $D(c) = a$, and $\{a, c\}$ is added to $E(T)$.

Step 3: Going into the **while** loop: $V(T) = \{a, b, c\}$, $E(T) = \{\{a, b\}, \{a, c\}\}$



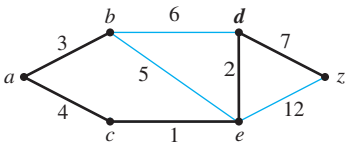
During iteration:
$F = \{d, e\}$, $L(d) = 9$, $L(e) = 5$
$L(e)$ becomes 5 because *ace*, which has length 5, is a shorter path to e than *abe*, which has length 8.
Since $L(e) < L(d)$, e is added to $V(T)$, $D(e) = c$, and $\{c, e\}$ is added to $E(T)$.

Step 4: Going into the **while** loop: $V(T) = \{a, b, c, e\}$, $E(T) = \{\{a, b\}, \{a, c\}, \{c, e\}\}$



During iteration:
$F = \{d, z\}$, $L(d) = 7$, $L(z) = 17$
$L(d)$ becomes 7 because *aced*, which has length 7, is a shorter path to d than *abd*, which has length 9.
Since $L(d) < L(z)$, d is added to $V(T)$, $D(d) = e$, and $\{e, d\}$ is added to $E(T)$.

Step 5: Going into the **while** loop: $V(T) = \{a, b, c, e, d\}$, $E(T) = \{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}\}$



During iteration:
$F = \{z\}$, $L(z) = 14$
$L(z)$ becomes 14 because *acedz*, which has length 14, is a shorter path to d than *abdz*, which has length 17.
Since z is the only vertex in F, its label is a minimum, and so z is added to $V(T)$, $D(z) = d$, and $\{d, z\}$ is added to $E(T)$.

Execution of the algorithm terminates at this point because $z \in V(T)$. The shortest path from a to z has length $L(z) = 14$.

Keeping track of the steps in a table is a convenient way to show the action of the algorithm. Table 10.6.1 does this for the graph in Example 10.6.5.

TABLE 10.6.1

Step	$V(T)$	$E(T)$	F	$L(a)$	$L(b)$	$L(c)$	$L(d)$	$L(e)$	$L(z)$
0	$\{a\}$	$\varnothing$	$\{a\}$	**0**	∞	∞	∞	∞	∞
1	$\{a\}$	$\varnothing$	$\{b, c\}$	0	**3**	4	∞	∞	∞
2	$\{a, b\}$	$\{\{a, b\}\}$	$\{c, d, e\}$	0	3	**4**	9	8	∞
3	$\{a, b, c\}$	$\{\{a, b\}, \{a, c\}\}$	$\{d, e\}$	0	3	4	9	**5**	∞
4	$\{a, b, c, e\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}\}$	$\{d, z\}$	0	3	4	**7**	5	17
5	$\{a, b, c, e, d\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}\}$	$\{z\}$	0	3	4	7	5	**14**
6	$\{a, b, c, e, d, z\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}, \{e, z\}\}$							

In step 1, $D(b) = a$; in step 2, $D(c) = a$; in step 3, $D(e) = c$; in step 4, $D(d) = e$; and in step 5, $D(z) = e$. Working backward gives the vertices in the shortest path. Because $D(z) = d$, $D(d) = e$, $D(e) = c$, and $D(c) = a$, the shortest path from a to z is $acedz$. ■

It is clear that Dijkstra's algorithm keeps adding vertices to T until it has added z. The proof of the following theorem shows that when the algorithm terminates, the label for z, $L(z)$, is the length of the shortest path to z from a.

Theorem 10.6.4 Correctness of Dijkstra's Algorithm

When a connected, simple graph with a positive weight for every edge is input to Dijkstra's algorithm with starting vertex a and ending vertex z, the output is the length of a shortest path from a to z.

Proof:

Let G be a connected, weighted graph with no loops or parallel edges and with a positive weight for every edge. Let T be the graph built up by Dijkstra's algorithm, and for each vertex u in G, let $L(u)$ be the label given by the algorithm to vertex u. For each integer $n \geq 0$, let the property $P(n)$ be the sentence

> After the nth iteration of the while loop in Dijkstra's algorithm, (1) T is a tree, and (2) for every vertex v in T, $L(v)$ is the length of a shortest path in G from a to v. ←$P(n)$

We will show by mathematical induction that $P(n)$ is true for each integer n from 0 through the termination of the algorithm.

Show that P(0) is true: When $n = 0$, the graph T is a tree because it is defined to consist only of the vertex a and no edges. In addition, $L(a)$ is the length of the shortest path from a to a because the initial value of $L(a)$ is 0.

Show that for every integer k ≥ 0, if P(k) is true then P(k + 1) is also true: Let k be any integer with $k \geq 0$ and suppose that

> After the kth iteration of the while loop in Dijkstra's algorithm, (1) T is a tree, and (2) for every vertex v in T, $L(v)$ is the length of a shortest path in G from a to v. ←$P(k)$ inductive hypothesis

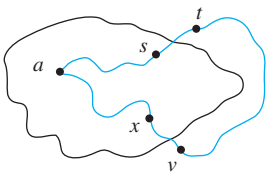
(continued on page 756)

We must show that

> After the $(k+1)$st iteration of the **while** loop in Dijkstra's algorithm, (1) T is a tree, and (2) for every vertex v in T, $L(v)$ is the length of a shortest path in G from a to v. ←$P(k+1)$

Suppose that after the $(k+1)$st iteration of the **while** loop in Dikjstra's algorithm, the vertex v and edge $\{x, v\}$ have been added to T, where x is in $V(T)$. Clearly the new value of T is a tree because adding a new vertex to a tree along with the edge leading to it neither creates a circuit nor disconnects the tree. By inductive hypothesis, for each vertex y that is in the tree before the addition of v, $L(y)$ is the length of a shortest path from a to y. So it remains only to show that $L(v)$ is the length of a shortest path from a to v.

Now, according to the algorithm, the final value of $L(v) = L(x) + w(x, v)$. Consider *any* shortest path from a to v, and let $\{s, t\}$ be the first edge in this path to leave T, where $s \in V(T)$ and $t \notin V(T)$. This situation is illustrated below.



Let $LSP(a, v)$ be the length of a shortest path from a to v, and let $LSP(a, s)$ be the length of a shortest path from a to s. Observe that

$$LSP(a, v) \geq LSP(a, s) + w(s, t)$$ because the path from t to v has length ≥ 0

$$\geq L(s) + w(s, t)$$ by inductive hypothesis because s is a vertex in T

$$\geq L(x) + w(x, v)$$ t is in the fringe of the tree, and so if $L(s) + w(s, t)$ were less than $L(x) + w(x, v)$ then t would have been added to T instead of r.

On the other hand,

$$L(x) + w(x, v) \geq LSP(a, v)$$ because $L(x) + w(x, v)$ is the length of a path from a to v and so it is greater than or equal to the length of the shortest path from a to v.

Because both $LSP(a, v) \geq L(x) + w(x, v)$ and $L(x) + w(x, v) \geq LSP(a, v)$, we have that

$$LSP(a, v) = L(x) + w(x, v).$$

And since it is also the case that

$$L(v) = L(x) + w(x, v),$$

we conclude that

$$L(v) = LSP(a, v).$$

Therefore, $L(v)$ is the length of a shortest path from a to v, which completes the proof by mathematical induction.

The algorithm terminates as soon as z is in T, and, since we have proved that the label of every vertex in the tree gives the length of the shortest path to it from a, then, in particular, $L(z)$ is the length of a shortest path from a to z.

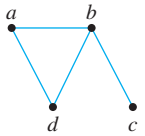
TEST YOURSELF

1. A spanning tree for a graph G is _____.
2. A weighted graph is a graph for which _____, and the total weight of the graph is _____.
3. A minimum spanning tree for a connected, weighted graph is _____.
4. In Kruskal's algorithm, the edges of a connected, weighted graph are examined one by one in order of _____ starting with _____.
5. In Prim's algorithm, a minimum spanning tree is built by expanding outward from an _____ in a sequence of _____.
6. In Dijkstra's algorithm, a vertex is in the fringe if it is _____ vertex in the tree that is being built up.
7. At each stage of Dijkstra's algorithm, the vertex that is added to the tree is a vertex in the fringe whose label is a _____.

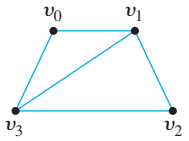
EXERCISE SET 10.6

Find all possible spanning trees for each of the graphs in 1 and 2.

1.

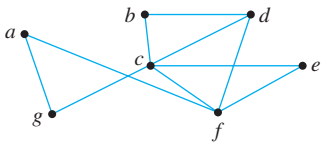


2.

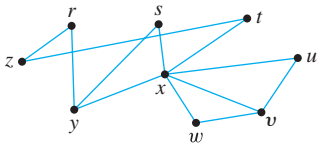


Find a spanning tree for each of the graphs in 3 and 4.

3.

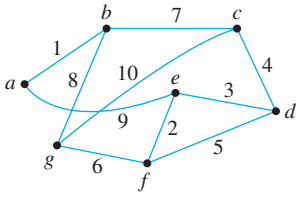


4.

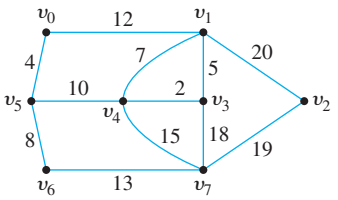


Use Kruskal's algorithm to find a minimum spanning tree for each of the graphs in 5 and 6. Indicate the order in which edges are added to form each tree.

5.



6.

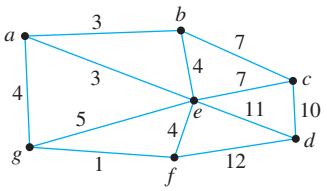


Use Prim's algorithm starting with vertex a or v_0 to find a minimum spanning tree for each of the graphs in 7 and 8. Indicate the order in which edges are added to form each tree.

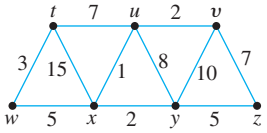
7. The graph of exercise 5. **8.** The graph of exercise 6.

For each of the graphs in 9 and 10, find all minimum spanning trees that can be obtained using (a) Kruskal's algorithm and (b) Prim's algorithm starting with vertex a or t. Indicate the order in which edges are added to form each tree.

9.

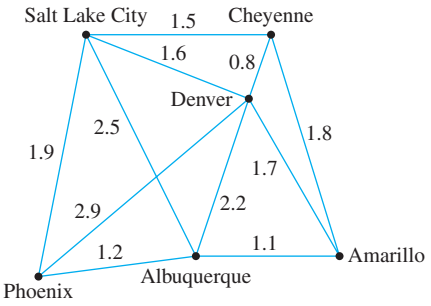


10.



11. A pipeline is to be built that will link six cities. The cost (in hundreds of millions of dollars)

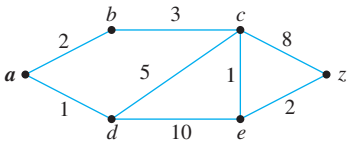
of constructing each potential link depends on distance and terrain and is shown in the weighted graph below. Find a system of pipelines to connect all the cities and yet minimize the total cost.



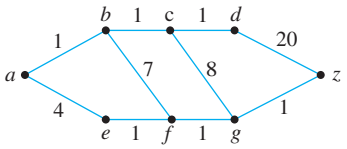
12. Use Dijkstra's algorithm for the airline route system of Figure 10.6.3 to find the shortest distance from Nashville to Minneapolis. Make a table similar to Table 10.6.1 to show the action of the algorithm.

Use Dijkstra's algorithm to find the shortest path from *a* to *z* for each of the graphs in 13–16. In each case make tables similar to Table 10.6.1 to show the action of the algorithm.

13.



14.



15. The graph of exercise 9 with $a = a$ and $z = f$

16. The graph of exercise 10 with $a = u$ and $z = w$

17. Prove part (2) of Proposition 10.6.1: Any two spanning trees for a graph have the same number of edges.

18. Given any two distinct vertices of a tree, there exists a unique path from one to the other.

a. Give an informal justification for the above statement.

*** b.** Write a formal proof of the above statement.

19. Prove that if G is a graph with spanning tree T and e is an edge of G that is not in T, then the graph obtained by adding e to T contains one and only one set of edges that forms a circuit.

20. Suppose G is a connected graph and T is a circuit-free subgraph of G. Suppose also that if any edge e of G not in T is added to T, the resulting graph contains a circuit. Prove that T is a spanning tree for G.

21. a. Suppose T_1 and T_2 are two different spanning trees for a graph G. Must T_1 and T_2 have an edge in common? Prove or give a counterexample.

b. Suppose that the graph G in part (a) is simple. Must T_1 and T_2 have an edge in common? Prove or give a counterexample.

***H* 22.** Prove that an edge e is contained in every spanning tree for a connected graph G if, and only if, removal of e disconnects G.

23. Consider the spanning trees T_1 and T_2 in the proof of Theorem 10.6.3. Prove that $w(T_2) \leq w(T_1)$.

24. Suppose that T is a minimum spanning tree for a connected, weighted graph G and that G contains an edge e (not a loop) that is not in T. Let v and w be the endpoints of e. By exercise 18 there is a unique path in T from v to w. Let e' be any edge of this path. Prove that $w(e') \leq w(e)$.

***H* 25.** Prove that if G is a connected, weighted graph and e is an edge of G (not a loop) that has smaller weight than any other edge of G, then e is in every minimum spanning tree for G.

*** 26.** If G is a connected, weighted graph and no two edges of G have the same weight, does there exist a unique minimum spanning tree for G? Use the result of exercise 19 to help justify your answer.

*** 27.** Prove that if G is a connected, weighted graph and e is an edge of G that (1) has greater weight than any other edge of G and (2) is in a circuit of G, then there is no minimum spanning tree T for G such that e is in T.

28. Suppose a disconnected graph is input to Kruskal's algorithm. What will be the output?

29. Suppose a disconnected graph is input to Prim's algorithm. What will be the output?

30. Modify Algorithm 10.6.3 so that the output consists of the sequence of edges in the shortest path from a to z.

31. Prove that if a connected, weighted graph G is input to Algorithm 10.6.4 (shown below), the output is a minimum spanning tree for G.

Algorithm 10.6.4

Input: *G [a connected graph]*

Algorithm Body:

1. $T := G$.

2. $E :=$ the set of all edges of G, $m :=$ the number of edges of G.

3. while $(m > 0)$

3a. Find an edge e in E that has maximal weight.
3b. Remove e from E and set $m := m - 1$.
3c. if the subgraph obtained when e is removed from the edge set of T is connected **then** remove e from the edge set of T

end while

Output: *T [a minimum spanning tree for G]*

ANSWERS FOR TEST YOURSELF

1. a subgraph of G that contains every vertex of G and is a tree. **2.** each edge has an associated positive real number weight; the sum of the weights of all the edges of the graph **3.** a spanning tree that has the least possible total weight compared to all other spanning trees for the graph **4.** weight; an edge of least weight **5.** initial vertex; adjacent vertices and edges **6.** adjacent to a **7.** minimum among all those in the fringe

CHAPTER 11 ANALYSIS OF ALGORITHM EFFICIENCY

Bettmann/Getty Images

René Descartes (1596–1650)

In 1637 the French mathematician and philosopher René Descartes published his great philosophical work *Discourse on Method*. An appendix to this work, called "Geometry," laid the foundation for the subject of analytic geometry, in which geometric methods are applied to the study of algebraic objects, such as functions, equations, and inequalities, and algebraic methods are used to study geometric objects, such as straight lines, circles, and half-planes.

The analytic geometry of Descartes provides the foundation for the main topic of this chapter: analyzing algorithm efficiency using the big-O, big-Omega, and big-Theta notations. In Section 11.1 we briefly discuss certain properties of graphs of real-valued functions of a real variable that are needed to understand these notations. In Section 11.2 we define the notations, discuss why they are useful in the analysis of algorithms, and apply them to power and polynomial functions. Then in Section 11.3 we show how to use the notations to compare the efficiencies of various algorithms designed to do the same job. Because the analysis of algorithms often involves logarithmic and exponential functions, we develop the needed properties of these functions in Section 11.4 and use them to analyze several algorithms in Section 11.5.

11.1 Real-Valued Functions of a Real Variable and Their Graphs

The first precept was never to accept a thing as true until I knew it as such without a single doubt. —René Descartes, 1637

A **Cartesian plane** or **two-dimensional Cartesian coordinate system** is a pictorial representation of $\mathbf{R} \times \mathbf{R}$, obtained by setting up a one-to-one correspondence between ordered pairs of real numbers and points in a Euclidean plane. To obtain it, two perpendicular lines, called the **horizontal** and **vertical axes**, are drawn in the plane. Their point of intersection is called the **origin**, and a unit of distance is chosen for each axis. An ordered pair (x, y) of real numbers corresponds to the point P that lies $|x|$ units to the right or left of the vertical axis and $|y|$ units above or below the horizontal axis. On each axis the positive direction is marked with an arrow.

Definition

A **real-valued function of a real variable** is a function from one set of real numbers to another. If f is a real-valued function of a real variable, then for each real number x in the domain of f there is a unique corresponding real number $f(x)$. The **graph of f** is the set of all points (x, y) in the Cartesian coordinate plane with the property that x is in the domain of f and $y = f(x)$.

The definition of graph (see Figure 11.1.1) means that for each x in the domain of f:

$$y = f(x) \quad \Leftrightarrow \quad \text{the point } (x, y) \text{ lies on the graph of } f.$$

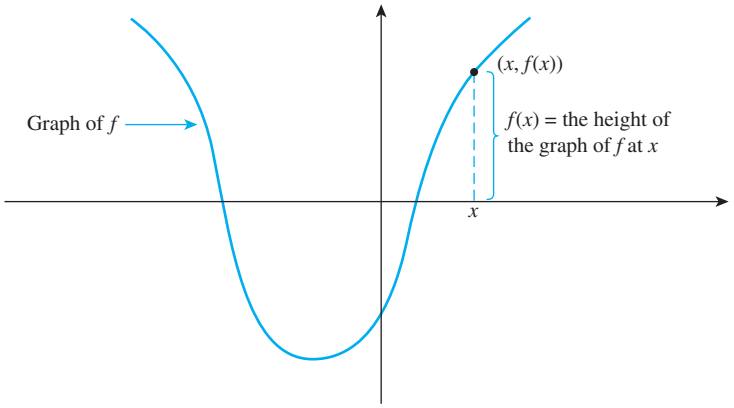


FIGURE 11.1.1 Graph of a Function f

Note that if $f(x)$ can be written as an algebraic expression in x, the graph of the function f is the same as the graph of the equation $y = f(x)$ where x is restricted to lie in the domain of f.

Power Functions

A function that sends a real number x to a particular power, x^a, is called a *power function*. For applications in computer science, we are almost invariably concerned with situations where x and a are nonnegative, and so we restrict our definition to these cases.

Definition

Let a be any nonnegative real number. Define p_a, the **power function with exponent a**, as follows:

$$p_a(x) = x^a \quad \text{for each nonnegative real number } x.$$

Example 11.1.1 **Graphs of Power Functions**

Sketch the graphs of the power functions p_0, $p_{1/2}$, p_1, and p_2 on the same coordinate axes.

Solution Because the power function with exponent zero satisfies $p_0(x) = x^0 = 1$ for every nonnegative number x,* all points of the form $(x, 1)$ lie on the graph of p_0 for every $x \geq 0$. So the graph is just a horizontal half-line of height 1 lying above the horizontal axis. Similarly, $p_1(x) = x$ for every nonnegative number x, and so the graph of p_1 consists of all points of the form (x, x) where x is nonnegative. The graph is therefore the half-line of slope 1 that emanates from (0, 0).

Since for each nonnegative number x, $p_{1/2}(x) = x^{1/2} = \sqrt{x}$, any point with coordinates $(x,\sqrt{x})$, where x is nonnegative, is on the graph of $p_{1/2}$. For instance, the graph of $p_{1/2}$ contains the points (0, 0), (1, 1), (4, 2), and (9, 3). Similarly, since $p_2(x) = x^2$, any point with

*As in Section 5.2 (see page 282), for simplicity we define $0^0 = 1$.

coordinates (x, x^2) lies on the graph of p_2. Thus, for instance, the graph of p_2 contains the points (0, 0), (1, 1), (2, 4), and (3, 9).

The graphs of all four functions are shown in Figure 11.1.2.

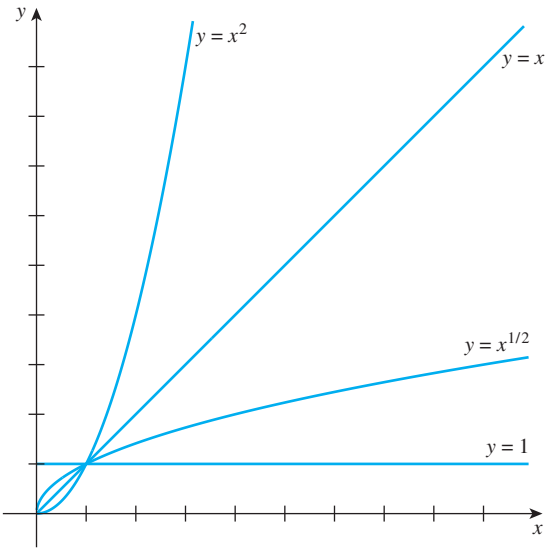


FIGURE 11.1.2 Graphs of Some Power Functions ■

The Floor Function

The floor and ceiling functions arise in many computer science contexts. Example 11.1.2 illustrates the graph of the floor function. In exercise 6 at the end of this section you are asked to draw the graph of the ceiling function.

Example 11.1.2 **Graph of the Floor Function**

Recall that each real number either is an integer itself or sits between two consecutive integers: For each real number x, there exists a unique integer n such that $n \le x < n + 1$. The floor of a number is the integer immediately to its left on the number line. More formally, the floor function F is defined by the rule

For each real number x,

$$\begin{aligned} F(x) &= \lfloor x \rfloor \\ &= \text{the greatest integer that is less than or equal to } x \\ &= \text{the unique integer } n \text{ such that } n \le x < n + 1. \end{aligned}$$

Sketch a graph of the floor function.

Solution If n is any integer, then for each real number x in the interval $n \le x < n + 1$, the floor of x, $\lfloor x \rfloor$, equals n. Thus on each such interval, the graph of the floor function is horizontal; for each x in the interval, the height of the graph is n.

It follows that the graph of the floor function consists of horizontal line segments, like a staircase, as shown in Figure 11.1.3. The open circles at the right-hand edge of each step are used to show that those points are *not* on the graph.

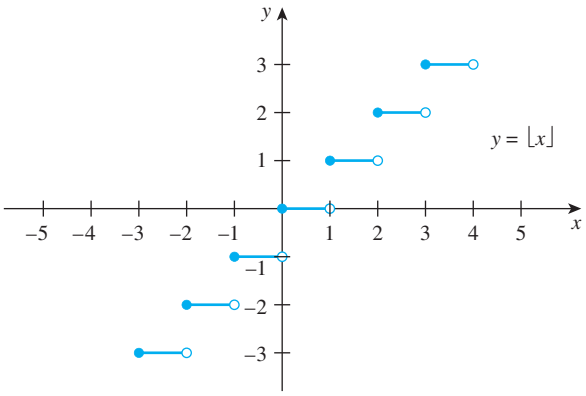
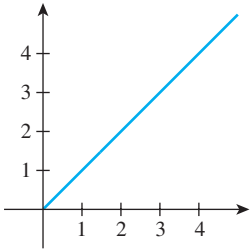


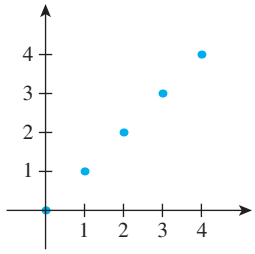
FIGURE 11.1.3 Graph of the Floor Function ■

Graphing Functions Defined on Sets of Integers

Many real-valued functions used in computer science are defined on sets of integers rather than on intervals of real numbers. But if you know what the graph of a function looks like when it is given by a formula on an interval of real numbers, you can obtain the graph of the function that is defined on the integers in the interval using the same formula by selecting only the points on the known graph whose first coordinates are integers. For instance, if f is the function defined by the same formula as the power function p_1 but having as its domain the set of nonnegative integers, then $f(n) = n$ for each nonnegative integer n. The graphs of p_1, reproduced from Example 11.1.2, and f are shown side-by-side below.



Graph of p_1 where $p_1(x) = x$ for each nonnegative real number x

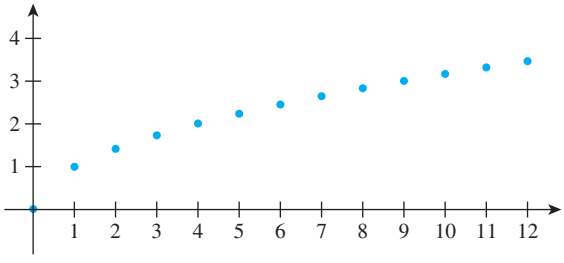


Graph of f where $f(n) = n$ for each nonnegative integer n

Example 11.1.3 **Graph of a Function Defined on a Set of Integers**

Consider an integer version of the power function $p_{1/2}$. In other words, define a function g by the formula $g(n)=n^{1/2}$ for each nonnegative integer n. Sketch the graph of g.

Solution Look back at the graph of $p_{1/2}$ in Figure 11.1.2. Draw the graph of g by reproducing only those points on the graph of $p_{1/2}$ with integer first coordinates. Thus for each nonnegative integer n, the point $(n, n^{1/2})$ is on the graph of g.



Graph of g where $g(n) = n^{1/2}$ for each nonnegative integer n ■

Graph of a Multiple of a Function

A *multiple* of a function is obtained by multiplying every value of the function by a fixed number. To understand the concept of O-notation, it is helpful to understand the relation between the graph of a function and the graph of a multiple of the function.

Definition

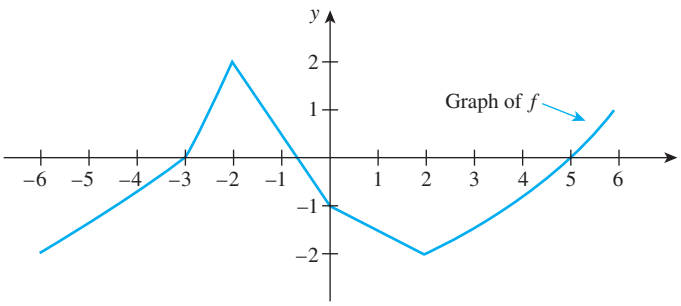
Let f be a real-valued function of a real variable and let M be any real number. The function Mf, called the **multiple of f by M** or **M times f**, is the real-valued function with the same domain as f that is defined by the rule

$$(Mf)(x) = M \cdot (f(x)) \quad \text{for each } x \in \text{domain of } f.$$

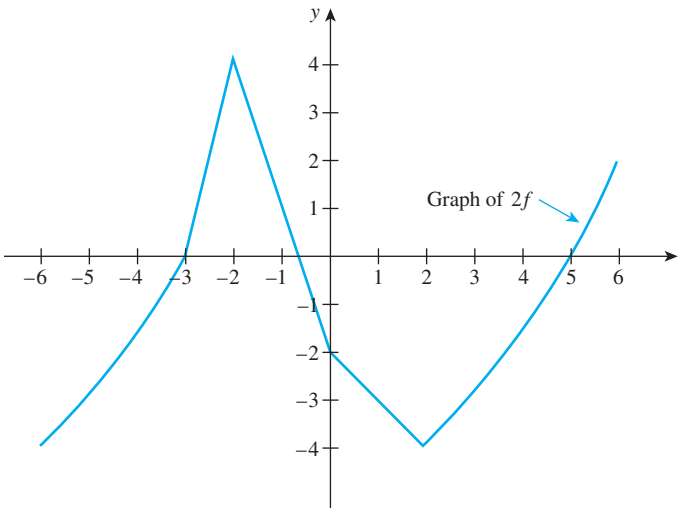
If the graph of a function is known, the graph of any multiple can easily be deduced. Specifically, if f is a function and M is a real number, the height of the graph of Mf at any real number x is M times the quantity $f(x)$. To sketch the graph of Mf from the graph of f, you plot the heights $M \cdot (f(x))$ on the basis of knowledge of M and visual inspection of the heights $f(x)$.

Example 11.1.4 **Graph of a Multiple of a Function**

Let f be the function whose graph is shown below. Sketch the graph of $2f$.



Solution At each real number x, you obtain the height of the graph of $2f$ by measuring the height of the graph of f at x and multiplying that number by 2. The result is the following graph. Note that the general shapes of f and $2f$ are very similar, but the graph of $2f$ is "stretched out": the "highs" are twice as high and the "lows" are twice as low.



■

Increasing and Decreasing Functions

Consider the *absolute value function*, A, which is defined as follows:

$$A(x) = |x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} \qquad \text{for each real number } x.$$

When $x \geq 0$, the graph of A is the same as the graph of $y = x$, the straight line with slope 1 that passes through the origin (0, 0). For $x < 0$, the graph of A is the same as the graph of $y = -x$, which is the straight line with slope -1 that passes through (0, 0). (See Figure 11.1.4.)

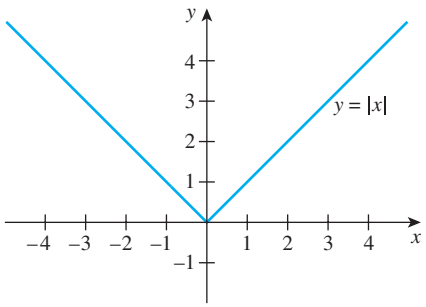


FIGURE 11.1.4 Graph of the Absolute Value Function

Note that as you trace from left to right along the graph to the left of the origin, the height of the graph continually *decreases*. For this reason, the absolute value function is said to be *decreasing* on the set of real numbers less than 0. On the other hand, as you trace from left to right along the graph to the right of the origin, the height of the graph continually *increases*. Consequently, the absolute value function is said to be *increasing* on the set of real numbers greater than 0.

Since the height of the graph of a function f at a point x is $f(x)$, these geometric concepts translate to the following analytic definition.

Definition

Let f be a real-valued function defined on a set of real numbers, and suppose the domain of f contains a set S. We say that f is **increasing on the set S** if, and only if,

$$\text{for all real numbers } x_1 \text{ and } x_2 \text{ in } S, \text{ if } x_1 < x_2 \text{ then } f(x_1) < f(x_2).$$

We say that f is **decreasing on the set S** if, and only if,

$$\text{for all real numbers } x_1 \text{ and } x_2 \text{ in } S, \text{ if } x_1 < x_2 \text{ then } f(x_1) > f(x_2).$$

We say that f is an **increasing** (or **decreasing**) **function** if, and only if, f is increasing (or decreasing) on its entire domain.

Figure 11.1.5 illustrates the analytic definitions of increasing and decreasing.

It follows almost immediately from the definitions that both increasing functions and decreasing functions are one-to-one. You are asked to show this in exercise 10 at the end of this section.

Example 11.1.5 **A Positive Multiple of an Increasing Function Is Increasing**

Suppose that f is a real-valued function of a real variable that is increasing on a set S of real numbers, and suppose M is any positive real number. Show that Mf is also increasing on S.

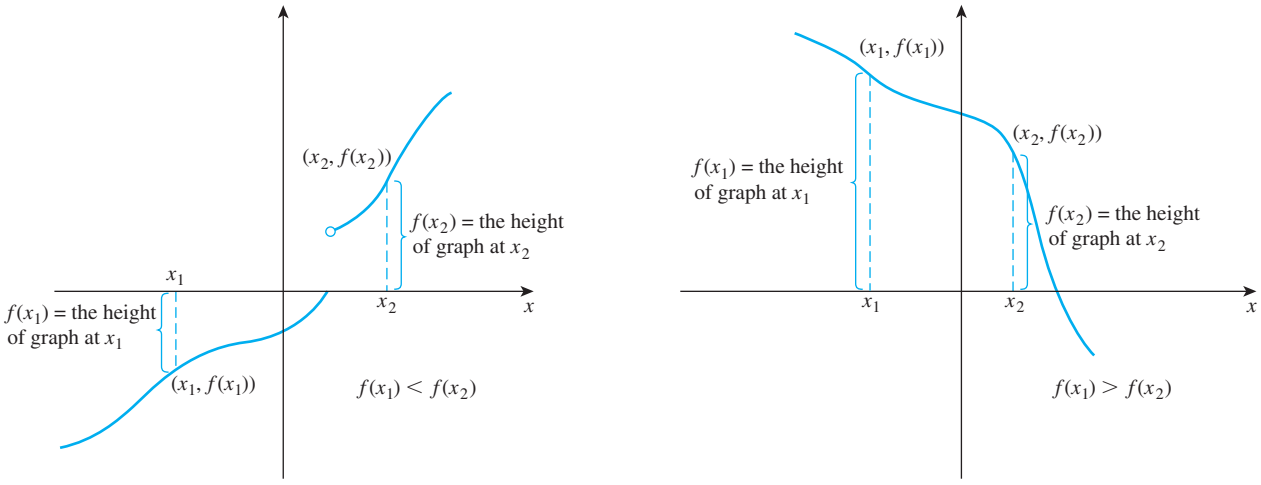


FIGURE 11.1.5

Solution Suppose x_1 and x_2 are particular but arbitrarily chosen elements of S such that

$$x_1 < x_2.$$

[We must show that $(Mf)(x_1) < (Mf)(x_2)$*.]* From the facts that $x_1 < x_2$ and f is increasing, it follows that

$$f(x_1) < f(x_2).$$

Then

$$Mf(x_1) < Mf(x_2),$$

since multiplying both sides of the inequality by a positive number does not change the direction of the inequality. Hence, by definition of Mf,

$$(Mf)(x_1) < (Mf)(x_2),$$

and, consequently, Mf is increasing on S. ■

It is also true that a positive multiple of a decreasing function is decreasing, that a negative multiple of an increasing function is decreasing, and that a negative multiple of a decreasing function is increasing. You are asked to prove these facts in exercises 24–26 at the end of this section.

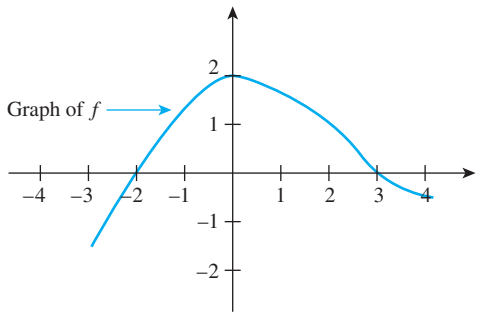
TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

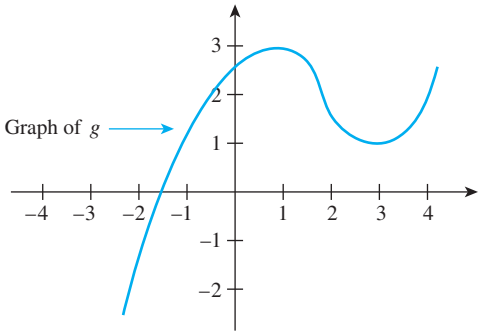
1. If f is a real-valued function of a real variable, then the domain and co-domain of f are both _____.
2. A point (x, y) lies on the graph of a real-valued function of a real variable f if, and only if, _____.
3. If a is any nonnegative real number, then the power function with exponent a, p_a, is defined by _____.
4. Given a function f: $\mathbf{R} \to \mathbf{R}$ and a real number M, the function Mf is defined by _____.
5. Given a function f: $\mathbf{R} \to \mathbf{R}$, to prove that f is increasing, you suppose that _____ and then you show that _____.
6. Given a function f: $\mathbf{R} \to \mathbf{R}$, to prove that f is decreasing, you suppose that _____ and then you show that _____.

EXERCISE SET 11.1*

1. The graph of a function f is shown below.
   - **a.** Is $f(0)$ positive or negative?
   - **b.** For what values of x does $f(x) = 0$?
   - **c.** Find approximate values for x_1 and x_2 so that $f(x) = f(x_2) = 1$ but $x_1 \neq x_2$.
   - **d.** Find an approximate value for x such that $f(x) = 1.5$.
   - **e.** As x increases from -3 to -1, do the values of f increase or decrease?
   - **f.** As x increases from 0 to 4, do the values of f increase or decrease?



2. The graph of a function g is shown below.
   - **a.** Is $g(0)$ positive or negative?
   - **b.** Find an approximate value of x so that $g(x) = 0$.
   - **c.** Find approximate values for x_1 and x_2 so that $g(x_1) = g(x_2) = 1$ but $x_1 \neq x_2$.
   - **d.** Find an approximate value for x such that $g(x) = -2$.
   - **e.** As x increases from -2 to 1, do the values of g increase or decrease?
   - **f.** As x increases from 1 to 3, do the values of g increase or decrease?



3. Sketch the graphs of the power functions $p_{1/3}$ and $p_{1/4}$ on the same set of axes. When $0 < x < 1$, which is greater: $x^{1/3}$ or $x^{1/4}$? When $x > 1$, which is greater: $x^{1/3}$ or $x^{1/4}$?

4. Sketch the graphs of the power functions p_3 and p_4 on the same set of axes. When $0 < x < 1$, which is greater: x^3 or x^4? When $x > 1$, which is greater: x^3 or x^4?

5. Sketch the graphs of $y = 2\lfloor x \rfloor$ and $y = \lfloor 2x \rfloor$ for each real number x. What can you conclude from these graphs?

Sketch a graph for each of the functions defined in 6–9 below.

6. $g(x) = \lceil x \rceil$ for each real number x (Recall that the ceiling of x, $\lceil x \rceil$, is the least integer that is greater than or equal to x. That is, $\lceil x \rceil =$ the unique integer n such that $n - 1 < x \leq n$.)

7. $h(x) = \lceil x \rceil - \lfloor x \rfloor$ for each real number x

8. $F(x) = \lfloor x^{1/2} \rfloor$ for each real number x

9. $G(x) = x - \lfloor x \rfloor$ for each real number x

In each of 10–13 a function is defined on a set of integers. Sketch a graph for each function.

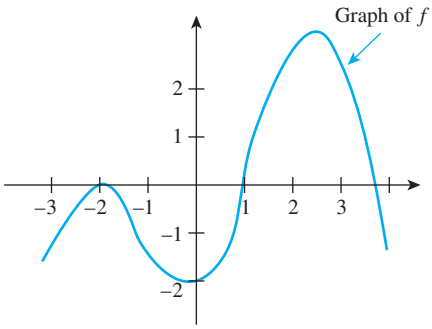
10. $f(n) = |n|$ for each integer n

11. $g(n) = (n/2) + 1$ for each integer n

12. $h(n) = \lfloor n/2 \rfloor$ for each integer $n \geq 0$

13. $k(n) = \lfloor n^{1/2} \rfloor$ for each integer $n \geq 0$

14. The graph of a function f is shown below. Find the intervals on which f is increasing and the intervals on which f is decreasing.



*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

15. Show that the function f: $\mathbf{R} \to \mathbf{R}$ defined by the formula $f(x) = 2x - 3$ is increasing on the set of real numbers.

16. Show that the function g: $\mathbf{R} \to \mathbf{R}$ defined by the formula $g(x) = -(x/3) + 1$ is decreasing on the set of real numbers.

17. Let h be the function from $\mathbf{R}$ to $\mathbf{R}$ defined by the formula $h(x) = x^2$ for each real number x

a. Show that h is decreasing on the set of real numbers less than zero.

b. Show that h is increasing on the set of real numbers greater than zero.

18. Let k: $\mathbf{R} \to \mathbf{R}$ be the function defined by the formula $k(x) = (x - 1)/x$ for each real number $x \neq 0$.

a. Show that k is increasing for every real number $x > 0$.

b. Is k increasing or decreasing for $x < 0$? Prove your answer.

19. Show that if a function f: $\mathbf{R} \to \mathbf{R}$ is increasing, then f is one-to-one.

20. Given real-valued functions f and g with the same domain D, the sum of f and g, denoted $f + g$, is defined as follows:

For each real number x, $(f + g)(x) = f(x) + g(x)$.

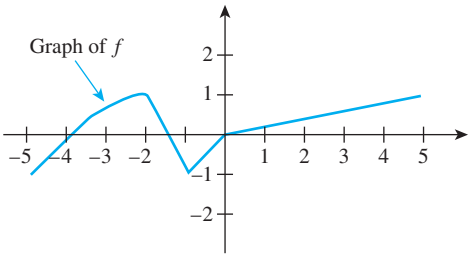
Show that if f and g are both increasing on a set S, then $f + g$ is also increasing on S.

21. **a.** Let m be any positive integer, and define $f(x) = x^m$ for each nonnegative real number x. Use the binomial theorem to show that f is an increasing function.

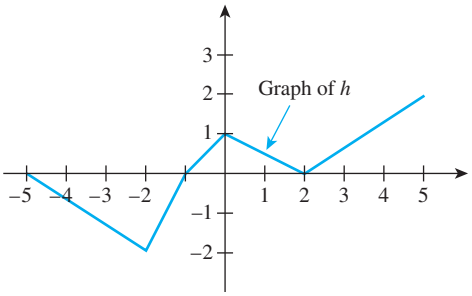
b. Let m and n be any positive integers, and let $g(x) = x^{m/n}$ for each nonnegative real number x. Prove that g is an increasing function.

Note: The results of exercise 21 are used in the exercises for Sections 11.2 and 11.4.

22. Let f be the function whose graph follows. Sketch the graph of $3f$.



23. Let h be the function whose graph is shown below. Sketch the graph of $2h$.



24. Let f be a real-valued function of a real variable. Show that if f is decreasing on a set S and if M is any positive real number, then Mf is decreasing on S.

25. Let f be a real-valued function of a real variable. Show that if f is increasing on a set S and if M is any negative real number, then Mf is decreasing on S.

26. Let f be a real-valued function of a real variable. Show that if f is decreasing on a set S and if M is any negative real number, then Mf is increasing on S.

In 27 and 28, functions f and g are defined. In each case sketch the graphs of f and $2g$ on the same set of axes and find a number x_0 so that $f(x) \leq 2g(x)$ for all $x > x_0$. You can find an exact value for x_0 by solving a quadratic equation, or you can find an approximate value for x_0 by using a graphing calculator or computer.

27. $f(x) = x^2 + 10x + 11$ and $g(x) = x^2$ for each real number $x \geq 0$

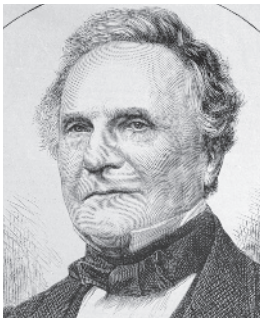
28. $f(x) = x^2 + 125x + 254$ and $g(x) = x^2$ for each real number $x \geq 0$

ANSWERS FOR TEST YOURSELF

1. sets of real numbers **2.** $y = f(x)$ **3.** $p_a(x) = x^a$ for each real number x **4.** $(Mf)(x) = M \cdot f(x)$ for each $x \in \mathbf{R}$ **5.** x_1 and x_2 are any real numbers such that $x_1 < x_2$; $f(x_1) < f(x_2)$ **6.** x_1 and x_2 are any real numbers such that $x_1 < x_2$; $f(x_1) > f(x_2)$

11.2 Big-O, Big-Omega, and Big-Theta Notations

As soon as an Analytical Engine exists, it will necessarily guide the future course of the science. Whenever any result is sought by its aid, the question will then arise—by what course of calculation can these results be arrived at by the machine in the shortest time? —Charles Babbage, 1864



Bettmann/Getty Images

Charles Babbage (1729–1871)

Understanding the relative efficiencies of computer algorithms is of much more than academic interest. In industrial and scientific settings, the choice of an efficient over an inefficient algorithm can save a great deal of money or even make the difference between being able or not being able to do a project at all.

The cost and feasibility of implementing a computer algorithm are most affected by the length of computer time and the amount of computer memory the algorithm requires. While both are important, this chapter concentrates on basic techniques for calculating time efficiency, which is usually the more significant of the two. Occasionally, however, one algorithm may make more efficient use of time but less efficient use of memory than another, forcing a trade-off based on the resources available to the user.

Charles Babbage's Analytical Engine was similar in many respects to a modern computer. The quotation at the beginning of this section shows that he anticipated the importance of analyzing the time efficiencies of computer algorithms almost a hundred years before the first computer was actually built.

The main objects of analysis in this chapter will be algorithms that take a data array and either search it to find a particular element or sort it into ascending or descending order. As a simple example, imagine running an algorithm to search an array of data for a particular element. In the best case the algorithm might happen to find the element in its very first step; in the worst case it might have to check every element before ending.

The best and worst cases cannot be predicted in advance because they depend on the nature of the data being processed, so, when comparing two algorithms, it is reasonable to want control over worst-case situations. Although the results involve approximation, analysis can reveal dramatic differences among algorithms designed to do the same job, at least for large data sets and in the worst cases. For example, the graph in Figure 11.2.1 gives a range of worst-case execution times for two algorithms used to sort sets of data: insertion sort and merge sort. As the length of the data set becomes larger and larger, the difference

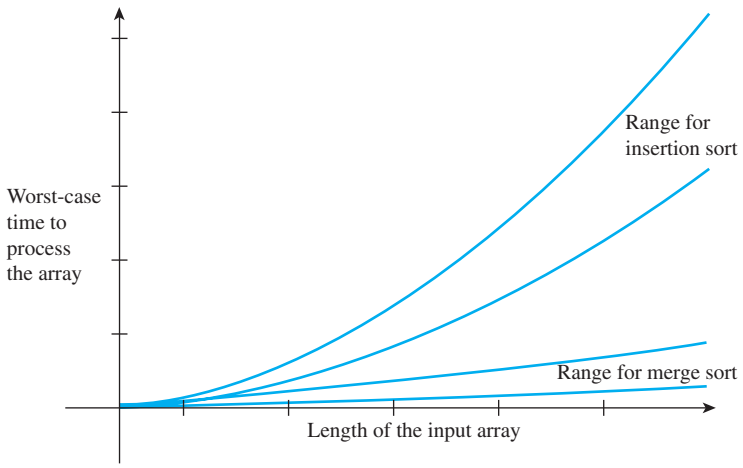


FIGURE 11.2.1

between the ranges becomes dramatically greater. For example, sorting a data set with 10 million items could take just a fraction of a second with merge sort but approximately 30 minutes with insertion sort.

The symbols Θ and Ω are the uppercase Greek letters theta and omega. The Θ-notation introduced in this section is determined by ranges such as those shown in Figure 11.2.1. It is related to two other notations: Ω-notation and O-notation. The oldest of the notations, O-notation (read "big-O notation"), was introduced by the German mathematician Paul Bachmann in 1894 in a book on analytic number theory, and it was the first to be used to compare efficiencies of algorithms. As you will see, however, using O-notation alone can produce ambiguous or even misleading results. As a response, in 1976 Donald Knuth, a pioneer in the analysis of algorithms, introduced the Ω- and Θ-notations so that the growth of functions could be compared with greater precision.

The idea of the notations is this: Suppose f and g are real-valued functions of an integer variable n and suppose $g(n) \geq 0$ for every integer n greater than some positive real number.

1. If, for sufficiently large values of n, the values of f are greater than those of a positive multiple of g, then f is of order *at least* g, written "$f(n)$ is $\Omega(g(n))$."
2. If, for sufficiently large values of n, the values of f are positive and less than those of a positive multiple of g, then f is of order *at most* g, written "$f(n)$ is $O(g(n))$."
3. If, for sufficiently large values of n, the values of f are bounded both above and below by those of positive multiples of g, then f is of order g, written "$f(n)$ is $\Theta(g(n))$."

These relationships are illustrated in Figure 11.2.2.

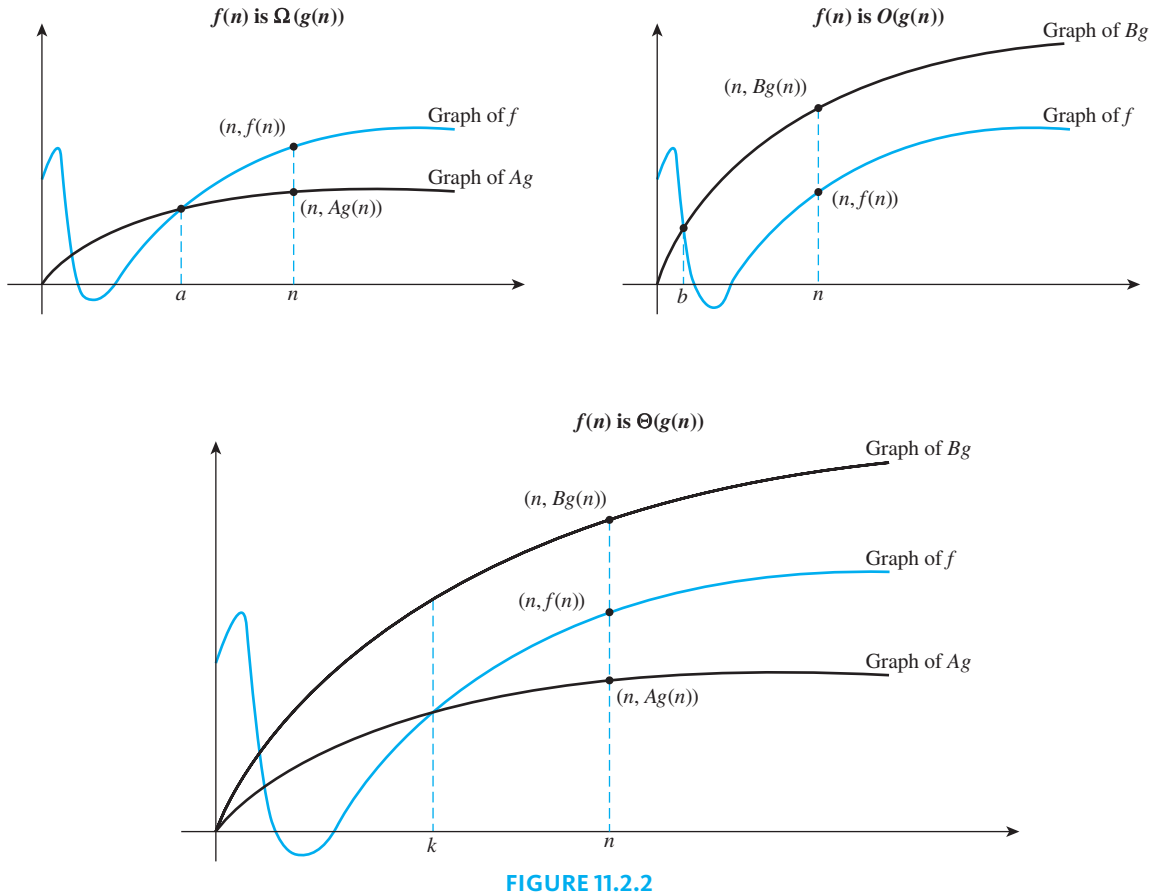


FIGURE 11.2.2

When they were originally defined, the order notations referred to functions defined on continuous intervals of real numbers rather than to functions defined on sets of integers. However, the important variable in the analysis of algorithm efficiency is the size of the problem the algorithm is designed to solve, which is an integer. For example, it might be the number of items in a data array to be sorted or the number of nodes in a graph where a minimum spanning tree is to be found.

Now when a function satisfies a property for all the real numbers in an interval, then it satisfies the property for all the integers in the interval, and the proofs in this chapter are valid if the phrase "for every real number x" is substituted in place of "for every integer n." Thus, although we restrict the discussion to functions defined on sets of integers, functions defined on intervals of real numbers are in the background. This is reflected in the fact that we show graphs as continuous curves rather than as sets of discrete points. As in Example 11.1.5, you can imagine how the graphs would look if they were defined for integer values only.

Definition

Let f and g be real-valued functions defined on the same set of nonnegative integers, with $g(n) \geq 0$ for every integer $n \geq r$, where r is a positive real number. Then

1. f **is of order at least** g, **written** $f(n)$ **is** $\Omega(g(n))$ (f of n is big-Omega of g of n), if, and only if, there exist positive real numbers A and $a \geq r$ such that
$$Ag(n) \leq f(n) \quad \text{for every integer } n \geq a.$$
2. f **is of order at most** g, **written** $f(n)$ **is** $O(g(n))$ (f of n is big-O of g of n), if, and only if, there exist positive real numbers B and $b \geq r$ such that
$$0 \leq f(n) \leq Bg(n) \quad \text{for every integer } n \geq b.$$
3. f **is of order** g, **written** $f(n)$ **is** $\Theta(g(n))$ (f of n is big-Theta of g of n), if, and only if, there exist positive real numbers A, B, and $k \geq r$ such that
$$Ag(n) \leq f(n) \leq Bg(n) \quad \text{for every integer } n \geq k.$$

Remark on Notation: In Section 7.1 we stated that we would carefully distinguish between a function f and a value $f(n)$ of the function. The traditional use of the order notation violates this principle. For instance, in the statement "$f(n)$ is $\Theta(g(n))$," the symbols $f(n)$ and $g(n)$ are understood to refer to the functions f and g defined by the expressions $f(n)$ and $g(n)$, respectively. For example, the statement
$$3n^2 + 4n + 5 \quad \text{is} \quad \Theta(n^2)$$
means that f is of order g where f and g are defined by the formulas $f(n) = 3n^2 + 4n + 5$ and $g(n) = n^2$ for every integer $n \geq 1$.

Example 11.2.1 **Translating to Θ-Notation**

Use Θ-notation to express the statement
$$4n^6 \leq 17n^6 - 45n^3 + 2n + 8 \leq 30n^6 \quad \text{for every integer } n \geq 3.$$

Solution Let $A = 4$, $B = 30$, and $k = 3$. Then the statement translates to
$$An^6 \leq 17n^6 - 45n^3 + 2n + 8 \leq Bn^6 \quad \text{for every integer } n \geq k.$$

So, by definition of Θ-notation,

$$17n^6 - 45n^3 + 2n + 8 \quad \text{is} \quad \Theta(n^6).$$

■

Example 11.2.2 **Translating to Ω- and O-Notations and Deducing Θ-Notation**

a. Use Ω-notation to express the statement

$$\frac{11}{4}n^2 \le 3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \quad \text{for every integer } n \ge 2.$$

b. Use O-notation to express the statement

$$0 \le 3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \le 6n^2 \quad \text{for every integer } n \ge 1.$$

c. Justify the statement: $3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2$ is $\Theta(n^2)$.

Solution

a. Let $A = \frac{11}{4}$ and $a = 2$. The statement in (a) translates to

$$An^2 \le 3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \quad \text{for every integer } n \ge a.$$

So, by definition of Ω-notation,

$$3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \quad \text{is} \quad \Omega(n^2).$$

b. Let $B = 6$ and $b = 1$. The statement in (b) translates to

$$0 \le 3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \le Bn^2 \quad \text{for every integer } n \ge b.$$

So, by definition of O-notation,

$$3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \quad \text{is} \quad O(n^2).$$

c. Let $A = \frac{11}{4}$, $a = 2$, $B = 6$, and $b = 1$, and let k be the larger of a and b. Then when $n \ge k$, both inequalities in parts (a) and (b) are satisfied, and so

$$An^2 \le 3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \le Bn^2 \quad \text{for every integer } n \ge k.$$

Hence by definition of Θ-notation,

$$3\left(\left\lfloor \frac{n}{4} \right\rfloor\right)^2 + 5n^2 \quad \text{is} \quad \Theta(n^2).$$

■

Part (c) of Example 11.2.2 illustrates the fact that if you know both that f is of order at most g and that f is of order at least g, then you may take k to be the larger of the numbers a and b promised in the definitions for big-Omega and big-O and conclude that f is of order g. Conversely, if f is of order g, then both a and b may be taken to be the number k promised in the definition for big-Theta to show that f is of order at most g and f is of order at least g. You are asked to summarize this discussion in a formal proof in exercise 19 at the end of this section.

Theorem 11.2.1 Relation among O-, Ω-, and Θ-Notations

If f and g are real-valued functions defined on the same set of nonnegative integers, and if $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$, where r is a positive real number,

then $f(n)$ is $\Theta(g(n))$ if, and only if, $f(n)$ is $\Omega(g(n))$ and $f(n)$ is $O(g(n))$.

Orders of Power Functions

The functions that are most commonly used for comparing algorithm efficiencies are power functions, such as $n^{1/2}$, n, n^2, and n^3, and combinations involving a power function and an exponential or logarithmic function, such as 2^n, $\log(n)$, $n \log(n)$, and $n^2 \log(n)$. These functions arise naturally in the analysis of algorithms, but, for large values of n, their sizes are dramatically different. In this section we focus on power functions, while in Section 11.4 we discuss functions that involve logarithms.

Observe that if

$$1 \leq n,$$

then

$$n \leq n^2 \qquad \text{by multiplying both sides by } n \text{ (which is positive)}$$

and so

$$n^2 \leq n^3 \qquad \text{by multiplying again by } n.$$

Thus if $n \geq 1$, then

$$1 \leq n \leq n^2 \leq n^3 \qquad \text{by transitivity of order.}$$

The following theorem generalizes this result. Exercises 46 and 47 at the end of this section provide an outline for the proof.

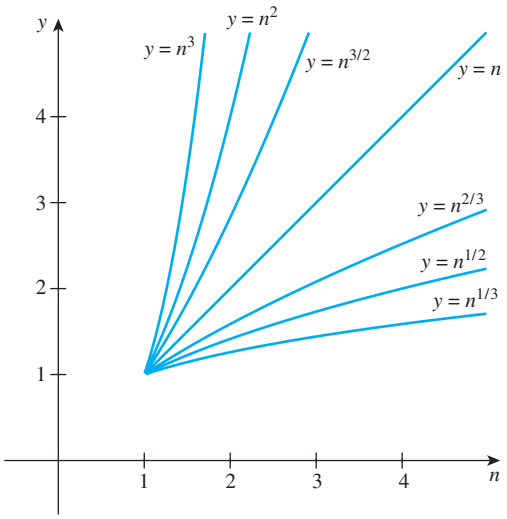
Theorem 11.2.2 For any positive rational numbers r and s and any integer $n \geq 1$,

$$\text{if } r \leq s, \quad \text{then} \quad n^r \leq n^s.$$

The relation among the graphs of various positive power functions of n for $n \geq 1$ is shown graphically in Figure 11.2.3.

Orders of Polynomial Functions

The following two examples show how to use Theorem 11.2.2 to find a big-Ω and a big-O for some polynomial functions.



If $r < s$, the graph of $y = n^r$ lies underneath the graph of $y = n^s$ for $n > 1$.

FIGURE 11.2.3 Graphs of Powers of n for $n \geq 1$

Example 11.2.3 **Finding a Big-Omega and a Big-*O* for a Polynomial Function with Nonnegative Coefficients**

a. Show that $15n^3 + 11n^2 + 9$ is $\Omega(n^3)$.

b. Without using part (a), show that $15n^3 + 11n^2 + 9$ is $O(n^3)$.

Solution

a. To show that $15n^3 + 11n^2 + 9$ is $\Omega(n^3)$, you need to show that $15n^3 + 11n^2 + 9$ is greater than or equal to a positive multiple of n^3 for all values of n that are sufficiently large. Now

$$15n^3 \leq 15n^3 + 11n^2 + 9 \quad \text{for every integer } n \geq 1$$

because when $n \geq 1$, $11n^2 + 9$ is positive. Thus you can let $A = 15$ and $a = 1$ to obtain

$$An^3 \leq 15n^3 + 11n^2 + 9 \quad \text{for every integer } n \geq a,$$

and conclude, by definition of Ω-notation, that $15n^3 + 11n^2 + 9$ is $\Omega(n^3)$.

b. To show that $15n^3 + 11n^2 + 9$ is $O(n^3)$, you need to show that $15n^3 + 11n^2 + 9$ is greater than or equal to 0 and less than or equal to some positive multiple of n^3 for all values of n that are sufficiently large. First note that because all terms of $15n^3 + 11n^2 + 9$ are positive,

$$0 \leq 15n^3 + 11n^2 + 9 \quad \text{for every integer } n \geq 1.$$

Next observe that for every integer $n \geq 1$,

$$15n^3 + 11n^2 + 9 \leq 15n^3 + 11n^3 + 9n^3$$

because, by Theorem 11.2.2, since $n \geq 1$, then $n \leq n^3$ and $1 \leq n^3$, and so $11n \leq 11n^3$ and $9 \leq 9n^3$

$$= 35n^3$$

because $15 + 11 + 9 = 35$.

Thus, by transitivity of order and equality,

$$0 \leq 15n^3 + 11n + 7 \leq 35n^3 \quad \text{for every integer } n \geq 1.$$

Let $B = 35$ and $b = 1$. Then

$$0 \leq 15n^3 + 11n^2 + 9 \leq Bn^3 \quad \text{for every integer } n \geq b,$$

and so, by definition of O-notation,

$$15n^3 + 11n^2 + 9 \text{ is } O(n^3).$$ ■

Example 11.2.4 **Finding a Big-Omega and a Big-O for a Polynomial Function with Some Negative Coefficients**

a. Show that $n^4 - 5n - 8$ is $\Omega(n^4)$.

b. Show that $n^4 - 5n - 8$ is $O(n^4)$.

Solution

a. To show that $n^4 - 5n - 8$ is $\Omega(n^4)$, you need to find positive real numbers A and a such that

$$An^4 \le n^4 - 5n - 8 \quad \text{for every integer } n \ge a.$$

Because $n^4 - 5n - 8$ contains negative terms, you need to use a different technique from the one illustrated in Example 11.2.3(a). Two methods are shown below. The first relies on ad hoc calculations and the second describes a general procedure.

Method 1 (Using ad hoc calculations): Let $\Leftrightarrow$ stand for the words "if, and only if," and observe that

$$(*) \qquad \frac{1}{2}n^4 \le n^4 - 5n - 8$$

$$\Leftrightarrow \qquad 5n + 8 \le \frac{1}{2}n^4$$

because adding or subtracting $5n + 8 - \frac{1}{2}n^4$ to both sides of an inequality preserves the direction of the inequality

$$(**) \Leftrightarrow \qquad \frac{10}{n^2} + \frac{16}{n^3} \le n$$

because dividing or multiplying both sides of an inequality by $2n^3$, which is positive, preserves the direction of the inequality.

Because all the inequalities are equivalent (that is, each inequality is true if, and only if, all the others are true), any value of n that makes inequality (**) true makes inequality (*) true also. A little trial and error shows that inequality (**) is true for every integer $n \ge 3$:

$$\text{If } n \ge 3, \text{ then } \frac{1}{n} \le \frac{1}{3}, \quad \text{and so} \quad \frac{10}{n^2} + \frac{16}{n^3} \le \frac{10}{3^2} + \frac{16}{3^3} = \frac{46}{27} < 2 < n.$$

Hence, by transitivity of order and equality,

$$\frac{10}{n^2} + \frac{16}{n^3} \le n \quad \text{for every integer } n \ge 3,$$

which is inequality (**). Therefore, inequality (*) is also true for $n \ge 3$:

$$\frac{1}{2}n^4 \le n^4 - 5n - 8 \quad \text{for every integer } n \ge 3.$$

Let $A = \frac{1}{2}$ and $a = 3$. Then

$$An^4 \le n^4 - 5n - 8 \quad \text{for every integer } n \ge a,$$

and so, by definition of Ω-notation, $n^4 - 5n - 8$ is $\Omega(n^4)$.

Method 2 (Using a general procedure):

Let m be a nonnegative integer, let $P(n)$ be a polynomial of degree m, and suppose the coefficient a_m of n^m is positive.

To find big-Omega for $P(n)$: Let $A = \frac{1}{2}a_m$, and let a be the number obtained as follows:

1. Find the sum of the absolute values of all the coefficients of $P(n)$ except for a_m.
2. Multiply the result of step 1 by $\dfrac{2}{a_m}$.
3. Let a be the larger of the number 1 and the result of step 2.

Show that $An^m \leq P(n)$ for every integer $n \geq a$.

To use the general procedure to show that $n^4 - 5n - 8$ is $\Omega(n^4)$, observe that the coefficient of its highest power is 1 and the sum of the absolute values of its other coefficients is $|-5| + |-8|$. Thus you would take

$$A = \frac{1}{2} \quad \text{and} \quad a = \frac{2}{1}(|-5| + |-8|)$$

and note that

$$a = \frac{2}{1}(|-5| + |-8|) = 26, \quad \text{which is greater than 1.}$$

Requiring $n \geq a$ means that

$$n \geq \frac{2}{1}(|-5| + |-8|),$$

and multiplying both sides by $\frac{1}{2}n^3$ gives

$$\begin{aligned} \frac{1}{2}n^4 &\geq (|-5| + |-8|)n^3 \\ &= 5n^3 + 8n^3 \\ &\geq 5n + 8 \end{aligned}$$

because $n \geq 1$ and so $5n^3 \geq 5n$ and $8n^3 \geq 8$.

Hence, by transitivity of order and equality,

$$\frac{1}{2}n^4 \geq 5n + 8 \quad \text{for every integer } n \geq a.$$

Subtracting the right-hand side from the left-hand side and adding $\frac{1}{2}n^4$ to both sides gives

$$n^4 - 5n - 8 \geq \frac{1}{2}n^4 \quad \text{for every integer } n \geq a.$$

Thus since $A = \frac{1}{2}$,

$$n^4 - 5n - 8 \geq An^4 \quad \text{for every integer } n \geq a,$$

and so, by definition of Ω-notation, $n^4 - 5n - 8$ is $\Omega(n^4)$.

b. To show that $n^4 - 5n - 8$ is $O(n^4)$, observe that for every integer $n \geq 1$,

$$\begin{aligned} n^4 - 5n - 8 &\leq n^4 + 5n + 8 && \text{because when } n \geq 1,\ 5n + 8 \text{ is positive} \\ &\leq n^4 + 5n^4 + 8n^4 && \text{by Theorem 11.2.2, since } n \geq 1, \text{ then } n \leq n^4 \\ & && \text{and } 1 \leq n^4, \text{ and so } 5n \leq 5n^4 \text{ and } 8 \leq 8n^4 \\ &= 14n^4 && \text{because } 1 + 5 + 8 = 14. \end{aligned}$$

Thus, by transitivity of order and equality,

$$n^4 - 5n - 8 \leq 14n^4 \quad \text{for every integer } n \geq 1.$$

In addition, by part (a)

$$\frac{1}{2}n^4 \leq n^4 - 5n - 8 \quad \text{for every integer } n \geq 3,$$

so since $0 \leq \frac{1}{2}n^4$, transitivity of order gives that

$$0 \leq n^4 - 5n - 8 \leq 14n^4 \quad \text{for every integer } n \geq 3.$$

Let $B = 14$ and $b = 3$. Then

$$0 \leq n^4 - 5n - 8 \leq Bn^4 \quad \text{for every integer } n \geq b,$$

and hence, by definition of O-notation, $n^4 - 5n - 8$ is $O(n^4)$. ■

The results of Examples 11.2.3 and 11.2.4 can be used to find big-Thetas for $15n^3 + 11n^2 + 9$ and $n^4 - 5n - 8$.

Example 11.2.5 **Finding a Big-Theta for a Polynomial Function**

a. Show that $15n^3 + 11n^2 + 9$ is $\Theta(n^3)$.

b. Show that $n^4 - 5n - 8$ is $\Theta(n^4)$.

Solution

a. By Example 11.2.3, $15n^3 + 11n^2 + 9$ is $O(n^3)$ and by Example 11.2.4, $15n^3 + 11n^2 + 9$ is $\Omega(n^3)$. Thus by Theorem 11.2.1, $15n^3 + 11n^2 + 9$ is $\Theta(n^3)$.

b. By Example 11.2.4, $n^4 - 5n - 8$ is both $\Omega(n^4)$ and $O(n^4)$. Thus, by Theorem 11.2.1, $n^4 - 5n - 8$ is $\Theta(n^4)$. ■

Theorem 11.2.3 A Limit on What Can Be Inferred from Big-O

For any function f and positive real numbers r and s with $r < s$,

$$\text{if } f(n) \text{ is } O(n^r) \text{ then } f(n) \text{ is } O(n^s).$$

Proof: Suppose r and s are real numbers with $r < s$ and f is a function such that $f(n)$ is $O(n^r)$. By definition of O-notation, there exist positive real numbers B and b such that

$$0 \leq f(n) \leq Bn^r \quad \text{for every integer } n \geq b.$$

(continued on page 778)

Now by Theorem 11.2.2,

$$Bn^r \le Bn^s \quad \text{for every integer } n \ge 1.$$

Let b_1 be the larger of b and 1. Then

$$0 \le f(n) \le Bn^s \quad \text{for every integer } n \ge b_1,$$

and thus $f(n)$ is $O(n^s)$.

It follows from Theorem 11.2.3 that knowing a function is big-O of another function gives only partial information about how the function behaves.

Example 11.2.6 **A Caution about O-notation**

Suppose a person finds that $f(n)$ is $O(n^5)$ and that $g(n)$ is $O(n^4)$. Because $4 < 5$, this person might conclude that the graph of g lies below the graph of f for large values of n. Show that this is not necessarily the case by showing that there exist functions f and g such that $f(n)$ is $O(n^5)$ and $g(n)$ is $O(n^4)$, yet for large values of n the graph of f lies below, not above, the graph of g.

Solution Let $f(n) = 15n^3 + 11n^2 + 9$ and $g(n) = n^4 - 5n - 8$. Since $f(n)$ is $O(n^3)$, it follows from Theorem 11.2.3 that $f(n)$ is $O(n^5)$. Also by Example 11.2.3, $g(n)$ is $O(n^4)$. However, Figure 11.2.4, which shows both f and g, suggests that for values of $n \ge 16$, the graph of g lies above the graph of f.

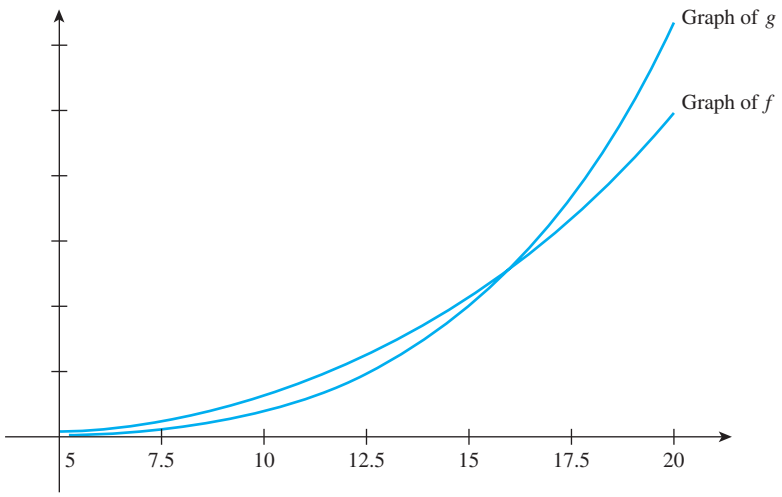


FIGURE 11.2.4

This result can be confirmed analytically by noting that

$$\begin{aligned}
(*) \qquad & g(n) \ge f(n) \\
\Leftrightarrow \quad & n^4 - 5n - 8 \ge 15n^3 + 11n^2 + 9 \\
\Leftrightarrow \quad & n^4 \ge 15n^3 + 11n^2 + 5n + 17 \\
(**) \Leftrightarrow \quad & n \ge 15 + \frac{11}{n} + \frac{5}{n^2} + \frac{17}{n^3}
\end{aligned}$$

So any value of n that satisfies inequality (**) also satisfies the inequality (*). Now when $n \geq 16$, then $\frac{1}{n} \leq \frac{1}{16}$, and so inequality (**) is satisfied because

$$15 + \frac{11}{n} + \frac{5}{n^2} + \frac{1}{n^3} \leq 15 + \frac{11}{16} + \frac{5}{16^2} + \frac{1}{16^3} \leq 16 \quad \text{for every integer } n \geq 16.$$

Therefore

$$n^4 - 5n - 8 \geq 15n^3 + 11n^2 + 9 \quad \text{for every integer } n \geq 16.$$

Thus it is possible to find bands around each graph so that the band around the graph of $g(n)$ lies entirely above the band around the graph of $f(n)$ for every integer $n \geq 16$. In fact, the second derivative test from calculus shows that $g(n)$ is growing at a faster rate than $f(n)$, which explains why the graph of $g(n)$ bends upward more steeply than the graph of $f(n)$. Readers who have studied calculus can check this result themselves. ■

A related feature of O-notation is illustrated by Example 11.2.7.

Example 11.2.7 **Showing That One Function Is Not Big-O of Some Other Function**

Let $g(n) = n^4 - 5n - 8$. By Example 11.2.4, $g(n)$ is $\Omega(n^4)$. Show that $g(n)$ is not $O(n^r)$ for any positive real number $r < 4$.

Solution

Suppose by way of contradiction that there exists a positive real number r such that $r < 4$ and $g(n)$ is $O(n^r)$. Then there exist positive real numbers B and b such that

$$0 \leq g(n) \leq Bn^r \quad \text{for every integer } n \geq b.$$

Since it is also the case that $g(n)$ is $\Omega(n^4)$, there exist positive real numbers A and a such that

$$An^4 \leq g(n) \quad \text{for every integer } n \geq a.$$

Let t be the larger of a and b. Then

$$An^4 \leq g(n) \leq Bn^r \quad \text{for every integer } n \geq t.$$

Let $\Rightarrow$ stand for the words "which implies that." It follows from the inequalities above that for every integer $n \geq t$,

$$\begin{aligned}
& An^4 \leq Bn^r && \text{by transitivity of order} \\
\Rightarrow \quad & \frac{n^4}{n^r} \leq \frac{B}{A} && \text{by dividing both sides by } An^r \\
\Rightarrow \quad & n^{4-r} \leq \frac{B}{A} && \text{by algebra} \\
\Rightarrow \quad & n \leq \sqrt[4-r]{B/A} && \text{by taking the } (4-r)\text{th root of both sides. (*)}
\end{aligned}$$

Since $r < 4$, then $4 - r > 0$, which implies that $\sqrt[4-r]{B/A}$ is a fixed positive real number. But n can be greater than any fixed number, which implies that condition (*) is contradictory. In other words, the supposition results in a contradiction, and hence it is false. Therefore, for each positive real number r with $r < 4$, $g(n)$ is not $O(n^r)$. ■

The next theorem generalizes the result of Example 11.2.7. The proof can be modeled on the solution to Example 11.2.7 and is left as exercise 21 at the end of this section.

Theorem 11.2.4 Showing That a Big-*O* Relationship Does Not Hold

If f is a real-valued function defined on a set of nonnegative integers and $f(n)$ is $\Omega(n^m)$, where m is a positive integer, then $f(n)$ is not $O(n^p)$ for any positive real number $p < m$.

Because Θ-notation, unlike O-notation, gives "tight bounds" on function values, you can count on it to give precise results for comparing function growths. In Example 11.2.5 Θ-notations were found for $15n^3 + 11n^2 + 9$ and $n^4 - 5n - 8$. In both cases the order of the polynomial function was the power function corresponding to the highest power in the polynomial. The theorem on polynomial orders shows that this result is not an accident. The simplest proof uses the idea of limit from calculus and is included below. Exercise 25 at the end of the section asks for a proof based on the techniques from Example 11.2.4, which does not rely on calculus.

Theorem 11.2.5 On Polynomial Orders

If m is any integer with $m \geq 0$ and $a_0, a_1, a_2, \ldots, a_m$ are real numbers with $a_m > 0$, then $a_m n^m + a_{m-1} n^{m-1} + \cdots + a_1 n + a_0$ is $\Theta(n^m)$.

Proof (using limits): Suppose m is an integer with $m \geq 0$ and suppose $a_0, a_1, a_2, \ldots, a_m$ are real numbers with $a_m > 0$. Because $\lim_{n \to \infty} \left(\frac{1}{n^i}\right) = 0$ for every integer $i \geq 1$,

$$\begin{aligned}
&\lim_{n \to \infty} \left(\frac{a_m n^m + a_{m-1} n^{m-1} + a_{m-2} n^{m-2} + \cdots + a_1 n + a_0}{n^m} \right) \\
&\qquad = \lim_{n \to \infty} \left(a_m + \frac{a_{m-1}}{n} + \frac{a_{m-2}}{n^2} + \cdots + \frac{a_1}{n^{m-1}} + \frac{a_0}{n^m} \right) \\
&\qquad = a_m.
\end{aligned}$$

By definition of limit, this implies that for any real number $\varepsilon > 0$, there exists an integer K such that

$$a_m - \varepsilon < a_m + \frac{a_{m-1}}{n} + \frac{a_{m-2}}{n^2} + \cdots + \frac{a_1}{n^{m-1}} + \frac{a_0}{n^m} < a_m + \varepsilon \quad \text{for every integer } n > K.$$

In particular, when $\varepsilon = \frac{a_m}{2}$, there is an integer k such that

$$a_m - \frac{a_m}{2} < a_m + \frac{a_{m-1}}{n} + \frac{a_{m-2}}{n^2} + \cdots + \frac{a_1}{n^{m-1}} + \frac{a_0}{n^m} < a_m + \frac{a_m}{2} \quad \text{for every integer } n > k.$$

Combining like terms and multiplying all parts of the inequality by n^m gives that

$$\left(\frac{a_m}{2}\right) n^m < a_m n^m + a_{m-1} n^{m-1} + \cdots + a_1 n + a_0 < \left(\frac{3a_m}{2}\right) n^m \quad \text{for every integer } n > k.$$

Let $A = \frac{a_m}{2}$ and $B = \frac{3a_m}{2}$. Then

$$An^m < a_m n^m + a_{m-1} n^{m-1} + \cdots + a_1, n + a_0 < Bn^m \quad \text{for every integer } n > k.$$

Therefore, by definition of Θ-notation,

$$a_m n^m + a_{m-1} n^{m-1} + \cdots + a_1 n + a_0 \text{ is } \Theta(n^m).$$

Example 11.2.8 **Calculating Polynomial Orders Using the Theorem on Polynomial Orders**

Use the theorem on polynomial orders to find orders for the functions given by the following formulas.

a. $f(n) = 7n^5 + 5n^3 - n + 4$ for each positive integer n.

b. $g(n) = \dfrac{(n-1)(n+1)}{4}$ for each positive integer n.

Solution

a. By direct application of the theorem on polynomial orders, $7n^5 + 5n^3 - n + 4$ is $\Theta(n^5)$.

b. $$\begin{aligned} g(n) &= \frac{(n-1)(n+1)}{4} \\ &= \frac{1}{4}(n^2 - 1) \\ &= \frac{1}{4}n^2 - \frac{1}{4} \quad \text{by algebra.} \end{aligned}$$

Thus $g(n)$ is $\Theta(n^2)$ ■

Example 11.2.9 **An Order for the Sum of the First *n* Integers**

Sums of the form $1 + 2 + 3 + \cdots + n$ arise in the analysis of computer algorithms such as selection sort. Show that for a positive integer variable n,

$$1 + 2 + 3 + \cdots + n \text{ is } \Theta(n^2).$$

Solution According to the formula for the sum of the first n integers (see Theorem 5.2.1), for each positive integer n,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Now

$$\frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n \quad \text{by basic algebra.}$$

And, by the theorem on polynomial orders,

$$\frac{1}{2}n^2 + \frac{1}{2}n \quad \text{is} \quad \Theta(n^2).$$

Hence

$$1 + 2 + 3 + \cdots + n \quad \text{is} \quad \Theta(n^2).$$ ■

We end this section by stating some theorems that give useful properties of order notations. These will be applied in Section 11.4. Two sample proofs are given, with the rest being left to the exercises at the end of the section.

Theorem 11.2.6 Reciprocal Relationship between Ω- and *O*-notations

Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$. Then:

a. If $f(n)$ is $\Omega(g(n))$, then $g(n)$ is $O(f(n))$.

b. If $g(n)$ is $O(f(n))$, then $f(n)$ is $\Omega(g(n))$.

Theorem 11.2.7 Reflexive, Symmetric, and Transitive Properties of Θ-notation

Let f, g, and h be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$, $g(n) \geq 0$ and $h(n) \geq 0$, for every integer $n \geq r$. Then:

a. $f(n)$ is $\Theta(f(n))$.

b. If $f(n)$ is $\Theta(g(n))$, then $g(n)$ is $\Theta(f(n))$.

c. If $f(n)$ is $\Theta(g(n))$ and $g(n)$ is $\Theta(h(n))$, then $f(n)$ is $\Theta(h(n))$.

Theorem 11.2.8 Effect of Constants on Order Notations

Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$.

Then for every positive real number c:

a. If $f(n)$ is $\Omega(g(n))$, then $cf(n)$ is $\Omega(g(n))$;

b. If $f(n)$ is $O(g(n))$, then $cf(n)$ is $O(g(n))$;

c. If $f(n)$ is $\Theta(g(n))$, then $cf(n)$ is $\Theta(g(n))$.

Theorem 11.2.9 Orders of Sums and Products of Functions

Let f_1, f_2, g_1, and g_2 be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f_1(n) \geq 0$, $f_2(n) \geq 0$, $g_1(n) \geq 0$, and $g_2(n) \geq 0$ for every integer $n \geq r$. Then:

a. If $f_1(n)$ is $\Theta(g(n))$ and $f_2(n)$ is $\Theta(g(n))$, then $(f_1(n) + f_2(n))$ is $\Theta(g(n))$.

b. If $f_1(n)$ is $\Theta(g_1(n))$ and $f_2(n)$ is $\Theta(g_2(n))$, then $(f_1(n)f_2(n))$ is $\Theta(g_1(n)g_2(n))$.

c. If $f_1(n)$ is $\Theta(g_1(n))$ and $f_2(n)$ is $\Theta(g_2(n))$ and if there is a real number s so that $g_1(n) \leq g_2(n)$ for every integer $n \geq s$, then $(f_1(n) + f_2(n))$ is $\Theta(g_2(n))$.

Proof of Theorem 11.2.6(a)

Let f and g be real-valued functions defined on the same set of nonnegative integers and suppose there is a positive real number r such that $g(n) \geq 0$ for every integer $n \geq r$. Suppose also that $f(n)$ is $\Omega(g(n))$. We will show that $g(n)$ is $O(f(n))$. By definition of Ω-notation, there are positive real numbers A and a such that $a \geq r$, and

$$Ag(n) \leq f(n) \quad \text{for every integer } n \geq a.$$

Divide both sides by A to obtain

$$g(n) \leq \frac{1}{A} f(n) \qquad \text{for every integer } n \geq a.$$

In addition, since $a \geq r$,

$$0 \leq g(n) \qquad \text{for every integer } n \geq a.$$

Let $B = 1/A$ and $b = a$. Then B and b are positive real numbers and

$$0 \leq g(n) \leq Bf(n) \qquad \text{for every integer } n \geq b,$$

and so $g(n)$ is $O(f(n))$ by definition of O-notation *[as was to be shown]*.

Proof of Theorem 11.2.7(c)

Suppose f, g, and h are real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$, $g(n) \geq 0$, and $h(n) \geq 0$, for every integer $n \geq r$. Suppose also that $f(n)$ is $\Theta(g(n))$ and $g(n)$ is $\Theta(h(n))$. We will show that $f(n)$ is $\Theta(h(n))$. By definition of Θ-notation, there exist positive real numbers A_1, B_1, k_1, A_2, B_2, and k_2 with $k_1 \geq r$ and $k_2 \geq r$, and

$$A_1 g(n) \leq f(n) \leq B_1 g(n) \qquad \text{for every integer } n \geq k_1$$

and

$$A_2 h(n) \leq g(n) \leq B_2 h(n) \qquad \text{for every integer } n \geq k_2.$$

Let $A = A_1 A_2$, $B = B_1 B_2$, and $k = \max(k_1, k_2)$. Then, by transitivity of order and equality, for every integer $n \geq k$,

$$Ah(n) = A_1(A_2 h(n)) \leq A_1 g(n) \leq f(n) \leq B_1 g(n) \leq B_1(B_2 h(n)) = Bh(n),$$

and so, by definition of Θ-notation, $f(n)$ is $\Theta(h(n))$ *[as was to be shown]*.

TEST YOURSELF

1. A sentence of the form "$Ag(n) \leq f(n)$ for every $n \geq a$" translates into Ω-notation as _____.
2. A sentence of the form "$0 \leq f(n) \leq Bg(n)$ for every $n \geq b$" translates into O-notation as _____.
3. A sentence of the form "$Ag(n) \leq f(n) \leq Bg(n)$ for every $n \geq k$" translates into Θ-notation as _____.
4. When $n \geq 1$, n _____ n^2 and n^2 _____ n^5.
5. According to the theorem on polynomial orders, if $p(n)$ is a polynomial in n, then $p(n)$ is $\Theta(n^m)$, where m is _____.
6. If n is a positive integer, then $1 + 2 + 3 + \cdots + n$ has order _____.

EXERCISE SET 11.2

1. The following is a formal definition for Ω-notation, written using quantifiers and variables: $f(n)$ is $\Omega(g(n))$ if, and only if, $\exists$ positive real numbers a and A such that $\forall\ n \geq a$,

$$Ag(n) \leq f(n).$$

a. Write the formal negation for the definition using the symbols $\forall$ and $\exists$.
b. Restate the negation less formally without using the symbols $\forall$ and $\exists$ or the words "for any," "for every," or "there exists."

2. The following is a formal definition for O-notation, written using quantifiers and variables: $f(n)$ is $O(g(n))$ if, and only if, $\exists$ positive real numbers b and B such that $\forall\ n \geq b$,

$$0 \leq f(n) \leq Bg(n).$$

a. Write the formal negation for the definition using the symbols $\forall$ and $\exists$.
b. Restate the negation less formally without using the symbols $\forall$ and $\exists$ or the words "for any," "for every," or "there exists."

3. The following is a formal definition for Θ-notation, written using quantifiers and variables: $f(n)$ is $\Theta(g(n))$ if, and only if, $\exists$ positive real numbers k, A, and B such that $\forall\ n \geq k$,

$$Ag(n) \leq f(n) \leq Bg(n).$$

a. Write the formal negation for the definition using the symbols $\forall$ and $\exists$.
b. Restate the negation less formally without using the symbols $\forall$ and $\exists$ or the words "for any," "for every," or "there exists."

In 4–9, express each statement using Ω-, O-, or Θ-notation.

4. $\frac{1}{2}n \leq n - \left\lfloor \frac{n}{2} \right\rfloor + 1$ for every integer $n \geq 1$.
(Use Ω-notation.)

5. $0 \leq n - \left\lfloor \frac{n}{2} \right\rfloor + 1 \leq n$ for every integer $n \geq 3$.
(Use O-notation.)

6. $n^2 \leq 3n(n-2) \leq 4n^2$ for every integer $n \geq 3$.
(Use Θ-notation.)

7. $\frac{1}{2}n^2 \leq \frac{n(3n-2)}{2}$ for every integer $n \geq 3$.
(Use Ω-notation.)

8. $0 \leq \frac{n(3n-2)}{2} \leq n^2$ for every integer $n \geq 1$.
(Use O-notation.)

9. $\frac{n^3}{6} \leq n^2\left(\left\lceil \frac{n}{3} \right\rceil - 1\right) \leq n^3$ for every integer $n \geq 2$.
(Use Θ-notation.)

10. **a.** Show that for any integer $n \geq 1$, $0 \leq 2n^2 + 15n + 4 \leq 21n^2$.
b. Show that for any integer $n \geq 1$, $2n^2 \leq 2n^2 + 15n + 4$.
c. Sketch a graph to illustrate the results of parts (a) and (b).
d. Use the O- and Ω-notations to express the results of parts (a) and (b).
e. What can you deduce about the order of $2n^2 + 15n + 4$?

11. **a.** Show that for any integer $n \geq 1$, $0 \leq 23n^4 + 8n^2 + 4n \leq 35n^4$.
b. Show that for any integer $n \geq 1$, $23n^4 \leq 23n^4 + 8n^2 + 4n$.
c. Sketch a graph to illustrate the result of parts (a) and (b).
d. Use the O- and Ω-notations to express the results of parts (a) and (b).
e. What can you deduce about the order of $23n^4 + 8n^2 + 4n$?

12. **a.** Show that for any integer $n \geq 1$, $0 \leq 7n^3 + 10n^2 + 3 \leq 20n^3$.
b. Show that for any integer $n \geq 1$, $7n^3 \leq 7n^3 + 10n^2 + 3$.
c. Sketch a graph to illustrate the result of parts (a) and (b).
d. Use the O- and Ω-notations to express the results of parts (a) and (b).
e. What can you deduce about the order of $7n^3 + 10n^2 + 3$?

13. Use the definition of Θ-notation to show that $5n^3 + 65n + 30$ is $\Theta(n^3)$.

14. Use the definition of Θ-notation to show that $n^2 + 100n + 88$ is $\Theta(n^2)$.

15. Use the definition of Θ-notation to show that $\left\lfloor n + \frac{1}{2} \right\rfloor$ is $\Theta(n)$.

16. Use the definition of Θ-notation to show that $\left\lceil n + \frac{1}{2} \right\rceil$ is $\Theta(n)$.

17. Use the definition of Θ-notation to show that $\left\lfloor \frac{n}{2} \right\rfloor$ is $\Theta(n)$. (*Hint:* Show that if $n \geq 4$, then $\frac{n}{2} - 1 \geq \frac{1}{4}n$.)

18. Prove Theorem 11.2.7(b): If f and g are real-valued functions defined on the same set of nonnegative integers and if $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$, where r is a positive real number, then if $f(n)$ is $\Theta(g(n))$, then $g(n)$ is $\Theta(f(n))$.

19. Prove Theorem 11.2.1: If f and g are real-valued functions defined on the same set of nonnegative integers and if $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$, where r is a positive real number, then $f(n)$ is $\Theta(g(n))$ if, and only if, $f(n)$ is $\Omega(g(n))$ and $f(n)$ is $O(g(n))$.

20. Without using Theorem 11.2.4 prove that n^5 is not $O(n^2)$.

21. Prove Theorem 11.2.4: If f is a real-valued function defined on a set of nonnegative integers and $f(n)$ is $\Omega(n^m)$, where m is a positive integer, then $f(n)$ is not $O(n^p)$ for any positive real number $p < m$.

22. a. Use one of the methods of Example 11.2.4 to show that $2n^4 - 90n^3 + 3$ is $\Omega(n^4)$.
b. Show that $2n^4 - 90n^3 + 3$ is $O(n^4)$.
c. Justify the conclusion that $2n^4 - 90n^3 + 3$ is $\Theta(n^4)$.

23. a. Use one of the methods of Example 11.2.4 to show that $\frac{1}{5}n^2 - 42n - 8$ is $\Omega(n^2)$.
b. Show that $\frac{1}{5}n^2 - 42n - 8$ is $O(n^2)$.
c. Justify the conclusion that $\frac{1}{5}n^2 - 42n - 8$ is $\Theta(n^2)$.

24. a. Use one of the methods of Example 11.2.4 to show that $\frac{1}{4}n^5 - 50n^3 + 3n + 12$ is $\Omega(n^5)$.
b. Show that $\frac{1}{4}n^5 - 50n^3 + 3n + 12$ is $O(n^5)$.
c. Justify the conclusion that $\frac{1}{4}n^5 - 50n^3 + 3n + 12$ is $\Theta(n^5)$.

25. Suppose $P(n) = a_m n^m + a_{m-1}n^{m-1} + \cdots + a_2 n^2 + a_1 n + a_0$, where all the coefficients $a_0, a_1, \ldots, a_m$ are real numbers and $a_m > 0$.
a. Prove that $P(n)$ is $\Omega(n^m)$ by using the general procedure described in Example 11.2.4.
b. Prove that $P(n)$ is $O(n^m)$.
c. Justify the conclusion that $P(n)$ is $\Theta(n^m)$.

Use the theorem on polynomial orders to prove each of the statements in 26–31.

26. $\frac{(n+1)(n-2)}{4}$ is $\Theta(n^2)$

27. $\frac{n}{3}(4n^2 - 1)$ is $\Theta(n^3)$

28. $\frac{n(n-1)}{2} + 3n$ is $\Theta(n^2)$

29. $\frac{n(n-1)(2n+1)}{6}$ is $\Theta(n^3)$

30. $\left[\frac{n(n+1)}{2}\right]^2$ is $\Theta(n^4)$

31. $2(n-1) + \frac{n(n+1)}{2} + 4\left(\frac{n(n-1)}{2}\right)$ is $\Theta(n^2)$

Prove each of the statements in 32–39. Use the theorem on polynomial orders and results from the theorems and exercises in Section 5.2 as appropriate.

32. $1^2 + 2^2 + 3^2 + \cdots + n^2$ is $\Theta(n^3)$

33. $1^3 + 2^3 + 3^3 + \cdots + n^3$ is $\Theta(n^4)$

34. $2 + 4 + 6 + \cdots + 2n$ is $\Theta(n^2)$

35. $5 + 10 + 15 + 20 + 25 + \cdots + 5n$ is $\Theta(n^2)$

36. $\sum_{i=1}^{n} (4i - 9)$ is $\Theta(n^2)$

37. $\sum_{k=1}^{n} (k + 3)$ is $\Theta(n^2)$

***H* 38.** $\sum_{i=1}^{n} i(i+1)$ is $\Theta(n^3)$

39. $\sum_{k=3}^{n} (k^2 - 2k)$ is $\Theta(n^3)$

40. a. Prove: If c is a positive real number and if f is a real-valued function defined on a set of nonnegative integers with $f(n) \geq 0$ for every integer n greater than or equal to some positive real number, then $cf(n)$ is $\Theta(f(n))$.
b. Use part (a) to show that $3n$ is $\Theta(n)$.

41. Prove: If c is a positive real number and $f(n) = c$ for every integer $n \geq 1$, then $f(n)$ is $\Theta(1)$.

42. What can you say about a function f with the property that $f(n)$ is $\Theta(1)$?

Use Theorems 11.2.5–11.2.9 and the results of exercises 15–17, 40, and 41 to justify the statements in 43–45.

43. $\left\lfloor \frac{n+1}{2} \right\rfloor + 3n$ is $\Theta(n)$

44. $\frac{n(n-1)}{2} + \left\lfloor \frac{n}{2} \right\rfloor + 1$ is $\Theta(n^2)$

45. $\left\lfloor \frac{n}{2} \right\rfloor + 4n + 3$ is $\Theta(n)$

46. a. Use mathematical induction to prove that if n is any integer with $n \geq 1$, then for every integer $m \geq 1$, $n^m \geq 1$.

b. Prove that if n is any integer with $n \geq 1$, then $n^r \leq n^s$ for all integers r and s with $r \leq s$.

47. a. Let x be any positive real number. Use mathematical induction to prove that for every integer $m \geq 1$, if $x \leq 1$ then $x^m \leq 1$.

***H* b.** Explain how it follows from part (a) that if x is any positive real number, then for every integer $m \geq 1$, if $x^m > 1$ then $x > 1$.

c. Explain how it follows from part (b) that if x is any positive real number, then for every integer $m \geq 1$, if $x > 1$ then $x^{1/m} > 1$.

d. Let p, q, r, and s be positive integers, and suppose $p/q > r/s$. Use part (c) and the result of exercise 40 to prove Theorem 11.2.2. In other words, show that for any integer n, if $n > 1$ then $n^{p/q} > n^{r/s}$.

48. Prove Theorem 11.2.6(b): If f and g are real-valued functions defined on the same set of nonnegative integers, and if there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$, and if $g(n)$ is $O(f(n))$, then $f(n)$ is $\Omega(g(n))$.

49. Prove Theorem 11.2.7(a): If f is a real-valued function defined on a set of nonnegative integers and there is a real number r such that $f(n) \geq 0$ for every integer $n \geq r$, then $f(n)$ is $\Theta(f(n))$.

50. Prove Theorem 11.2.8:

a. Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) > 0$ for every integer $n \geq r$. If $f(n)$ is $\Omega(g(n))$ and c is any positive real number, then $cf(n)$ is $\Omega(g(n))$.

b. Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$. If $f(n)$ is $O(g(n))$ and c is any positive real number, then $cf(n)$ is $O(g(n))$.

c. Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for every integer $n \geq r$. If $f(n)$ is $\Theta(g(n))$ and c is any positive real number, then $cf(n)$ is $\Theta(g(n))$.

51. Prove Theorem 11.2.9:

***H* a.** Let f_1, f_2, and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f_1(n) \geq 0$, $f_2(n) \geq 0$, and $g(n) \geq 0$ for every integer $n \geq r$. If $f_1(n)$ is $\Theta(g(n))$ and $f_2(n)$ is $\Theta(g(n))$, then $(f_1(n) + f_2(n))$ is $\Theta(g(n))$.

b. Let f_1, f_2, g_1, and g_2 be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f_1(n) \geq 0$, $f_2(n) \geq 0$, $g_1(n) \geq 0$, and $g_2(n) \geq 0$ for every integer $n \geq r$. If $f_1(n)$ is $\Theta(g_1(n))$ and $f_2(n)$ is $\Theta(g_2(n))$, then $(f_1(n)f_2(n))$ is $\Theta(g_1(n)g_2(n))$.

c. Let f_1, f_2, g_1, and g_2 be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f_1(n) \geq 0$, $f_2(n) \geq 0$, $g_1(n) \geq 0$, and $g_2(n) \geq 0$ for every integer $n \geq r$. If $f_1(n)$ is $\Theta(g_1(n))$ and $f_2(n)$ is $\Theta(g_2(n))$ and if there is a real number s so that $g_1(n) \leq g_2(n)$ for every integer $n \geq s$, then $(f_1(n) + f_2(n))$ is $\Theta(g_2(n))$.

ANSWERS FOR TEST YOURSELF

1. $f(n)$ is $\Omega(g(n))$ **2.** $f(n)$ is $O(g(n))$ **3.** $f(n)$ is $\Theta(g(n))$ **4.** $\leq$; $\leq$ **5.** the degree of $p(n)$ **6.** n^2

11.3 Application: Analysis of Algorithm Efficiency I

Science History Images/Alamy Stock Photo

Alan Turing
(1912–1954)

Note For more about the work of Alan Turing, see Sections 6.4 and 12.3.

It is convenient to have a measure of the amount of work involved in a computing process, even though it be a very crude one. . . . We might, for instance, count the number of additions, subtractions, multiplications, divisions, recording of numbers . . . *
—Alan Turing, 1948

Starting in the late 1940s a number of mathematicians and computer scientists contributed to developing formal techniques for analyzing computer algorithms. As indicated by the quotation at the beginning of this section, Alan Turing may have been the first to suggest a concrete way for doing this. In the early 1960s, Donald Knuth began the process of expanding upon his own work and the work of others into a series of volumes titled *The Art of Computer Programming*.† The first three volumes are in their third edition, a fourth volume is being published in parts, and the fifth through seventh volumes are in preparation. The books are providing a solid and extensive foundation for computer science that is both elegant and mathematically rigorous.

Bbva/Notimex/Newscom

Donald Knuth
(born 1938)

The Sequential Search Algorithm

The object of a search algorithm is to hunt through an array of data in an attempt to find a particular item x. In a sequential search, x is compared to the first item in the array, then to the second, then to the third, and so on. The search is stopped if a match is found at any stage. On the other hand, if the entire array is processed without finding a match, then x is not in the array. An example of a sequential search is shown diagrammatically in Figure 11.3.1.

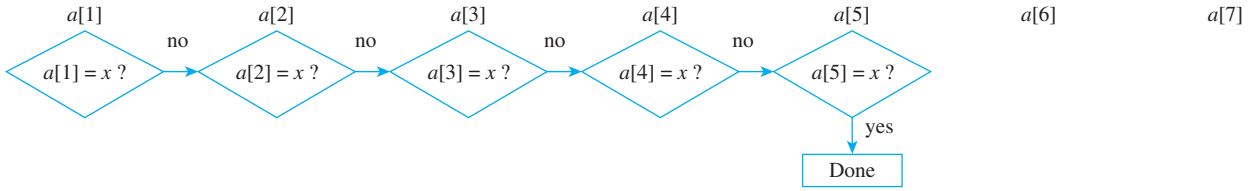


FIGURE 11.3.1 Sequential Search of $a[1], a[2], \ldots, a[7]$ for x where $x = a[5]$

Example 11.3.1 **Best-, Worst-, and Average-Case Orders for Sequential Search**

Find best, worst-, and average-case orders for the sequential search algorithm from among the set of power functions.

Solution Suppose the sequential search algorithm is applied to an input array $a[1], a[2], \ldots, a[n]$ to find an item x. In the best case, the algorithm requires only one comparison between x and the items in $a[1], a[2], \ldots, a[n]$. This occurs when x is the first item in the array.

**Quarterly Journal of Mechanics and Applied Mathematics*, vol. 1 (1948), pp. 287–308.

†Donald E. Knuth, *The Art of Computer Programming*, vol. 1: *Fundamental Algorithms*, 3rd ed. (1997); vol. 2: *Seminumerical Algorithms*, 3rd ed. (1997); vol. 3: *Searching and Sorting*, 2nd ed. (1998); vol. 4a: *Combinatorial Algorithms Part 1*, 1st ed. (2011); vol. 4: *Fascicle 6: Satisfiability*, 1st ed. (2015) (Addison-Wesley).

Thus in the best case, the sequential search algorithm is $\Theta(1)$. (Note that $\Theta(1) = \Theta(n^0)$.) In the worst case, however, the algorithm requires n comparisons. This occurs when $x = a[n]$ or when x does not appear in the array at all. Thus in the worst case, the sequential search algorithm is $\Theta(n)$. Finally, because x is as likely to be in the first half of the array as in the second half, the algorithm requires an average of $\frac{n}{2}$ comparisons. Since $\frac{n}{2}$ is $\Theta(n)$, the algorithm's average-case performance is also $\Theta(n)$. ■

Measuring the Efficiency of an Algorithm

Two aspects of algorithm efficiency are important: the amount of time required to execute the algorithm and the amount of memory space needed when it is run. In this chapter we introduce basic techniques for calculating time efficiency. Similar techniques exist for calculating space efficiency. Occasionally, one algorithm may make more efficient use of time but less efficient use of memory space than another, forcing a trade-off based on the resources available to the user.

How can the time efficiency of an algorithm be calculated? The answer depends on several factors. One is the size of the set of data that is input to the algorithm; for example, it takes longer for a sort algorithm to process 1,000,000 items than 100 items. Consequently, the execution time of an algorithm is generally expressed as a function of its input size.

Roughly speaking, the analysis of an algorithm for time efficiency begins by trying to count the number of elementary operations that must be performed when the algorithm is executed with an input of size n (in the best case, worst case, or average case). What is classified as an "elementary operation" may vary depending on the nature of the problem the algorithms being compared are designed to solve. For instance, to compare two algorithms for evaluating a polynomial, the crucial issue is the number of additions and multiplications that are needed, whereas to compare two algorithms for searching a list to find a particular element, the important distinction is the number of comparisons that are required. As is common, we will classify the following as **elementary operations**: addition, subtraction, multiplication, division, and comparisons that are indicated explicitly in an if-then statement using one of the relational symbols $<$, $\leq$, $>$, $\geq$, $=$, or $\neq$.

When algorithms are implemented in a particular programming language and run on a particular computer, some operations are executed faster than others, and, of course, there are differences in execution times from one machine to another. In certain practical situations these factors are taken into account when deciding which algorithm or which machine to use to solve a particular problem. In other cases, however, the machine is fixed, and rough estimates are all that are needed to determine the clear superiority of one algorithm over another. Since each elementary operation is executed in time no longer than the slowest, the time efficiency of an algorithm is approximately proportional to the number of elementary operations required to execute the algorithm.

Consider the example of two algorithms, A and B, designed to do a certain job. Suppose that for an input of size n, the number of elementary operations needed to perform algorithm A is between $10n$ and $20n$ (at least for large n), and the number of elementary operations needed to perform algorithm B is between $2n^2$ and $4n^2$. We say that in the worst case, algorithm A is $\Theta(n)$ (or has worst-case order n) and that in the worst case, algorithm B is $\Theta(n^2)$ (or has worst-case order n^2).

To compare the efficiencies of A and B, let *Max A* be the *maximum* number of operations needed to execute algorithm A, and let *Min B* be the *minimum* number of operations needed to execute algorithm B. Then *Max A* is $20n$ and *Max B* is $2n^2$. Table 11.3.1 shows the differences between algorithms A and B for larger and larger values of n.

TABLE 11.3.1 Number of Elementary Operations for Algorithms *A* and *B*

	Max A	*Min B*	*Max B − Max A*
n	$20n$	$2n^2$	$2n^2 - 20n$
1,000	20,000	2,000,000	1,980,000
10,000	200,000	200,000,000	199,800,000
1,000,000	20,000,000	2,000,000,000,000	1,999,980,000,000

For example, to accomplish a job with an input size of 1,000,000, algorithm *B* requires almost 2 trillion more elementary operations than algorithm *A*. One way to look at this is that algorithm *B* has to perform 100,000 operations for each single operation performed by algorithm *A*.

Definition

Let *A* be an algorithm.

1. Suppose the number of elementary operations performed when *A* is executed for an input of size n depends on n alone and not on the nature of the input data; say it equals $f(n)$. If $f(n)$ is $\Theta(g(n))$, we say that ***A* is $\Theta(g(n))$** or ***A* is of order $g(n)$**.
2. Suppose the number of elementary operations performed when *A* is executed for an input of size n depends on the nature of the input data as well as on n.
   a. Let $b(n)$ be the *minimum* number of elementary operations required to execute *A* for all possible input sets of size n. If $b(n)$ is $\Theta(g(n))$, we say that **in the best case, *A* is $\Theta(g(n))$** or ***A* has a best-case order of $g(n)$**.
   b. Let $w(n)$ be the *maximum* number of elementary operations required to execute *A* for all possible input sets of size n. If $w(n)$ is $\Theta(g(n))$, we say that **in the worst case, *A* is $\Theta(g(n))$** or ***A* has a worst-case order of $g(n)$**.

Some of the orders most commonly used to describe algorithm efficiencies are shown in Table 11.3.2. As you see from the table, differences between the orders of various types of algorithms can be more than astronomical. For instance, the time required for an algorithm of order 2^n to operate on a data set of size 100,000 is approximately $10^{30,076}$ times the estimated 13.8 billion years since the universe began (according to one theory of cosmology). On the other hand, an algorithm of order $\log_2 n$ needs at most a fraction of a second to process the same data set.

TABLE 11.3.2 Time Comparisons of Some Algorithm Orders

Approximate Time to Execute $f(n)$ Operations Assuming One Operation per Nanosecond*				
$f(n)$	$n = 10$	$n = 1{,}000$	$n = 100{,}000$	$n = 10{,}000{,}000$
$\log_2 n$	3.3×10^{-9} sec	10^{-8} sec	1.7×10^{-8} sec	2.3×10^{-8} sec
n	10^{-8} sec	10^{-6} sec	0.0001 sec	0.01 sec
$n \log_2 n$	3.3×10^{-8} sec	10^{-5} sec	0.0017 sec	0.23 sec
n^2	10^{-7} sec	0.001 sec	10 sec	27.8 hr
n^3	10^{-6} sec	1 sec	11.6 days	31,688 yr
2^n	10^{-6} sec	3.4×10^{284} yr	3.1×10^{30086} yr	2.9×10^{3010283} yr

*one nanosecond $= 10^{-9}$ second, one year $\cong$ 365.25 days

Example 11.3.2 Computing an Order of an Algorithm Segment

Assume n is a positive integer and consider the following algorithm segment:

$p := 0, x := 2$
for $i := 2$ **to** n
  $p := (p + i) \cdot x$
next i

a. Compute the actual number of elementary operations that are performed when this algorithm segment is executed.

b. Use the theorem on polynomial orders to find an order for this algorithm segment.

Solution

a. This algorithm segment has just one loop, which goes from 2 to n, and so there are as many iterations of the loop as there are integers from 2 to n, namely $n - 2 + 1 = n - 1$.* During each iteration, one multiplication and one addition are performed. Thus twice as many elementary operations are performed as there are iterations of the loop, and hence $2(n - 1) = 2n - 2$ elementary operations are performed when the algorithm segment is executed.

b. By the theorem on polynomial orders,

$$2n - 2 \quad \text{is} \quad \Theta(n),$$

and so this algorithm segment is $\Theta(n)$. ■

The next example looks at an algorithm segment that contains a nested loop.

Example 11.3.3 An Order for an Algorithm with a Nested Loop

Assume n is a positive integer and consider the following algorithm segment:

$s := 0$
for $i := 1$ **to** n
  for $j := 1$ **to** i
    if $\left\lfloor \frac{i}{j} \right\rfloor \cdot j = i$ **then** $s := s + 1$
  next j
next i

a. Compute the actual number of elementary operations that are performed when this algorithm segment is executed.

b. Use the theorem on polynomial orders to find an order for this algorithm segment.

Solution

a. Each iteration of the inner loop requires one division and one multiplication, so the total number of elementary operations is twice the number of iterations of the inner loop. Now the inner loop is iterated

one time when $i = 1$
two times when $i = 2$

*See "Counting the Elements of a List" in Section 9.1 to review this fact.

three times when $i = 3$

$\vdots$

n times when $i = n$.

You can see this easily if you construct a table that shows the values of i and j for which the statements in the inner loop are executed. Each column in the table represents one iteration.

i	1	2		3			4				⋯	n				
j	1	1	2	1	2	3	1	2	3	4	⋯	1	2	3	⋯	n
		1		2			3					4				n

Hence the total number of iterations of the inner loop is

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \qquad \text{by Theorem 5.2.1,}$$

and so the number of elementary operations performed is

$$2 \cdot \frac{n(n+1)}{2} = n(n+1).$$

An alternative method for computing the number of columns of the table uses an approach discussed in Example 9.6.3. Observe that the number of columns in the table is the same as the number of ways to place two $\times$'s in n categories, $1, 2, \ldots, n$, where the location of the $\times$'s indicates the values of i and j with $j \le i$. By Theorem 9.6.1, this number is

$$\binom{n-1+2}{2} = \binom{n+1}{2} = \frac{(n+1)!}{2!((n+1)-2)!} = \frac{(n+1)n(n-1)!}{2(n-1)!} = \frac{n(n+1)}{2}.$$

Although, for this example, the alternative method is more complicated than the one preceding it, it is simpler when the number of loop nestings exceeds two. (See exercise 19.)

b. By the theorem on polynomial orders, $n(n+1) = n^2 + n$ is $\Theta(n^2)$, and so this algorithm segment is $\Theta(n^2)$. ■

Example 11.3.4 **When the Number of Iterations Depends on the Floor Function**

Assume n is a positive integer and consider the following algorithm segment:

for $i := \lfloor n/2 \rfloor$ **to** n
  $a := n - i$
next i

a. Compute the actual number of elementary operations that are performed when this algorithm segment is executed.

b. Use the theorem on polynomial orders to find an order for this algorithm segment.

Solution

a. Each iteration of the loop requires one subtraction, and the loop is iterated as many times as there are integers from $\lfloor n/2 \rfloor$ to n, namely, $n - \lfloor \frac{n}{2} \rfloor + 1$ times. If n is even, then $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$, and so the number of elementary operations performed is

$$n - \left\lfloor \frac{n}{2} \right\rfloor + 1 = n - \frac{n}{2} + 1 = \frac{n+2}{2}.$$

If n is odd, then $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$, and so the number of elementary operations performed is

$$n - \left\lfloor \frac{n}{2} \right\rfloor + 1 = n - \frac{n-1}{2} + 1 = \frac{2n-(n-1)+2}{2} = \frac{n+3}{2}.$$

b. By the theorem on polynomial orders,

$$\frac{n+2}{2} \text{ is } \Theta(n) \quad \text{and} \quad \frac{n+3}{2} \text{ is } \Theta(n)$$

also. Hence, regardless of whether n is even or odd, this algorithm segment is $\Theta(n)$. ■

The Insertion Sort Algorithm

Insertion sort is an algorithm for arranging the items in an array into ascending order. Initially, the second item is compared to the first. If the second item is less than the first, their values are interchanged, and as a result the first two array items are in ascending order. The idea of the algorithm is gradually to lengthen the section of the array that is known to be in ascending order by inserting each subsequent array item into its correct position relative to the preceding ones. When the last item has been placed, the entire array is in ascending order.

Figure 11.3.2 illustrates the action of step k of insertion on an array $a[1], a[2], a[3], \ldots, a[n]$.

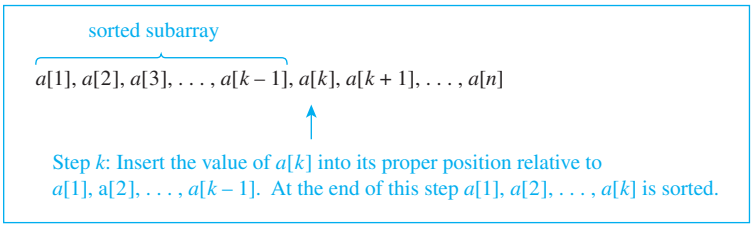


FIGURE 11.3.2 Step k of Insertion Sort

The following is a formal algorithm for insertion sort.

Algorithm 11.3.1 Insertion Sort

[The aim of this algorithm is to take an array $a[1], a[2], a[3], \ldots, a[n]$, *where* $n \geq 1$, *and reorder it. The output array is also denoted* $a[1], a[2], a[3], \ldots, a[n]$. *It has the same values as the input array, but they are in ascending order. In the kth step,* $a[1], a[2], a[3], \ldots, a[k-1]$ *is in ascending order, and* $a[k]$ *is inserted into the correct position with respect to it.]*

Input: n *[a positive integer],* $a[1], a[2], a[3], \ldots, a[n]$ *[an array of data items capable of being ordered]*

Algorithm Body:
for $k := 2$ **to** n

[Compare $a[k]$ to previous items in the array $a[1], a[2], a[3], \ldots, a[k-1]$, starting from the largest and moving downward. Whenever $a[k]$ is less than a preceding array item, the indexes of $a[k]$ and the preceding item are switched. As soon as $a[k]$ is greater than or equal to an array item, the value of $a[k]$ is left unchanged.]

```
    x := a[k]
    j := k − 1
    while (j ≠ 0)
      if x < a[j] then
          a[j + 1] := a[j]
          a[ j] := x
          j := j − 1
          else j := 0
      end if
    end while
next k
```

Output: $a[1], a[2], a[3], \ldots, a[n]$ *[in ascending order]*

Figure 11.3.3 shows the result of each step when insertion sort is applied to the particular array

$$a[1] = 6, \quad a[2] = 3, \quad a[3] = 5, \quad a[4] = 7, \quad a[5] = 2.$$

	a[1]	a[2]	a[3]	a[4]	a[5]
Initial	6	3	5	7	2
Result of step 1	3	6	5	7	2
Result of step 2	3	5	6	7	2
Result of step 3	3	5	6	7	2
Result of step 4	2	3	5	6	7

The top row of the table shows the initial values of the array, and the bottom row shows the final values. The result of each step is shown in a separate row. For each step, the sorted section of the array is shaded.

FIGURE 11.3.3 Action of Insertion Sort on an Array

Example 11.3.5 develops a trace table for the action of insertion sort on a particular array.

Example 11.3.5 **A Trace Table for Insertion Sort**

Construct a trace table showing the action of insertion sort on the array

$$a[1] = 6, a[2] = 3, a[3] = 5, a[4] = 7, a[5] = 2.$$

Solution

The first column shows the state of the variables before the first iteration of the **for-next** loop. When the **for-next** loop is first iterated, k is assigned the value 2; x the value of $a[2]$, which is 3; and j the value of $k - 1$, which is 1. Because $j \neq 0$, the **while** loop is entered and the condition for the **if-then-else** statement is tested. Because $a[1] > x$, then $a[2]$ is assigned the value of $a[1]$, which is 6, j is assigned the value of $j - 1$, which is 0, and $a[1]$ is

assigned the value of x, which is 3. The condition governing the **while** loop is tested again, but since $j = 0$, it is not satisfied, and so the **while** loop is not entered. Then the value of k is incremented by 1 (so that it equals 3), and the **for-next** loop is entered a second time. This process continues until the value of k has been incremented to 6. Because 6 is greater than the top value in the **for-next** loop, execution of the algorithm ceases, and the array items are in ascending order.

n	5											
***a*[1]**	6	3										2
***a*[2]**	3	6		5							2	3
***a*[3]**	5			6						2	5	
***a*[4]**	7								2	6		
***a*[5]**	2								7			
k	2		3			4		5				
x	3		5			7		2				
j	1	0	2	1	0	3	0	4	3	2	1	0

Example 11.3.6 **Finding a Worst-Case Order for Insertion Sort**

a. When insertion sort is applied to the array $a[1], a[2], a[3], \ldots, a[n]$, what is the maximum number of comparisons if those that control the **while** and **for-next** loops are included in the count?

b. Use the theorem on polynomial orders to find a worst-case order for insertion sort.

Solution

a. In each iteration of the **while** loop, one explicit comparison is made to test whether $a[j] > x$. During the time that $a[k]$ is put into position relative to $a[1], a[2], \ldots, a[k-1]$, the maximum number of attempted iterations of the **while** loop is k. This happens when $a[k]$ is less than every $a[1], a[2], \ldots, a[k-1]$ and results in $k-1$ comparisons. Then when the kth iteration is attempted, a comparison results in setting $j = 0$ and so the condition of the **while** loop is not satisfied. Thus the maximum number of comparisons for a given value of k is $k-1$. Now because k goes from 2 to n, the maximum total number of comparisons occurs when the items in the array are in reverse order, and it equals

$$\begin{aligned} 2+3+\cdots+n &= (1+2+3+\cdots+n)-1 && \text{by adding and subtracting 1} \\ &= \frac{n(n+1)}{2}-1 && \text{by Theorem 5.2.1} \\ &= \frac{n(n+1)}{2}-1 \\ &= \frac{1}{2}n^2+\frac{1}{2}n-1 && \text{by algebra.} \end{aligned}$$

b. By the theorem on polynomial orders, $\frac{1}{2}n^2+\frac{1}{2}n-1$ is $\Theta(n^2)$, and so the insertion sort algorithm has worst-case order $\Theta(n^2)$.

The definition of expected value that was introduced in Section 9.8 can be used to find an average-case order for insertion sort.

Example 11.3.7 **Finding an Average-Case Order for Insertion Sort**

a. What is the average number of comparisons that are performed when insertion sort is applied to the array $a[1], a[2], a[3], \ldots, a[n]$?

b. Use the theorem on polynomial orders to find an average-case order for insertion sort.

Solution

a. For any positive integer n, let E_n be the average, or expected, number of comparisons used to sort $a[1], a[2], \ldots, a[n]$ with insertion sort. Then for each integer $k = 2, 3, \ldots, n$,

$$\begin{bmatrix}\text{the expected number of}\\ \text{comparisons used to}\\ \text{sort } a[1], a[2], \ldots, a[k]\end{bmatrix}$$

$$= \begin{bmatrix}\text{the expected number of}\\ \text{comparisons used to}\\ \text{sort } a[1], a[2], \ldots, a[k-1]\end{bmatrix} + \begin{bmatrix}\text{the expected number of comparisons}\\ \text{used to place } a[k] \text{ into position}\\ \text{relative to } a[1], a[2], \ldots, a[k-1]\end{bmatrix}.$$

Thus

$$E_k = E_{k-1} + \begin{bmatrix}\text{the expected number of comparisons}\\ \text{used to place } a[k] \text{ into position}\\ \text{relative to } a[1], a[2], \ldots, a[k-1]\end{bmatrix}.$$

Also, $E_1 = 0$ because when there is just one item in the array, $n = 1$ and no iterations of the outer loop are performed.

Now at the time the **while** loop is used to place $a[k]$ relative to $a[1], a[2], \ldots, a[k-1]$, on average the value of $a[k]$ is equally likely to belong in any one of the first k positions. Thus the probability of its belonging in any particular position is $1/k$. If it actually belongs in position j, then $k-j+1$ comparisons will be used to move it, because there will be $k-j+1$ attempted iterations of the **while** loop and, as noted in Example 11.3.6, there is one comparison per attempted iteration.

According to the definition of expected value given in Section 9.8, the expected number of comparisons used to place $a[k]$ relative to $a[1], a[2], \ldots, a[k-1]$ is therefore

$$\begin{aligned}
\sum_{j=1}^{k} \frac{1}{k}(k-j+1) &= \frac{1}{k}\sum_{j=1}^{k}(k-j+1) && \text{by Theorem 5.1.1}\\
&= \frac{1}{k}[k+(k-1)+\cdots+3+2+1] && \text{by writing the summation in expanded form}\\
&= \frac{1}{k}\left(\frac{k(k+1)}{2}\right) && \text{by Theorem 5.2.1}\\
&= \frac{k+1}{2} && \text{by algebra.}
\end{aligned}$$

Hence

$$E_k = E_{k-1} + \frac{k+1}{2} \quad \text{for every integer } k \geq 2, \quad \text{and}$$

$$E_1 = 0.$$

In exercise 27 at the end of the section you are asked to solve this recurrence relation to show that

$$E_n = \frac{n^2 + 3n - 4}{4} \quad \text{for each integer } n \geq 1.$$

b. By the theorem on polynomial orders, $\frac{n^2 + 3n - 4}{4} = \frac{1}{4}n^2 + \frac{3}{4}n - 1$ is $\Theta(n^2)$, and so the average-case order of insertion sort is also $\Theta(n^2)$. ■

TEST YOURSELF

1. When an algorithm segment contains a nested **for-next** loop, you can find the number of times the loop will iterate by constructing a table in which each column represents _____.
2. In the worst case for an input array of length n, the sequential search algorithm has to look through _____ elements of the array before it terminates.
3. The worst-case order of the insertion sort algorithm is _____, and its average-case order is _____.

EXERCISE SET 11.3

1. Suppose a computer takes 1 nanosecond ($=10^{-9}$ second) to execute each operation. Approximately how long will it take the computer to execute the following numbers of operations? Convert your answers into seconds, minutes, hours, days, weeks, or years, as appropriate. For example, instead of 2^{50} nanoseconds, write 13 days.
   a. $\log_2 200$ **b.** 200 **c.** $200 \log_2 200$
   d. 200^2 **e.** 200^8 **f.** 2^{200}
2. Suppose an algorithm requires cn^2 operations when performed with an input of size n (where c is a constant).
   a. How many operations will be required when the input size is increased from m to $2m$ (where m is a positive integer)?
   b. By what factor will the number of operations increase when the input size is doubled?
   c. By what factor will the number of operations increase when the input size is increased by a factor of ten?
3. Suppose an algorithm requires cn^3 operations when performed with an input of size n (where c is a constant).
   a. How many operations will be required when the input size is increased from m to $2m$ (where m is a positive integer)?
   b. By what factor will the number of operations increase when the input size is doubled?
   c. By what factor will the number of operations increase when the input size is increased by a factor of ten?

Exercises 4–5 explore the fact that for relatively small values of n, algorithms with larger orders can be more efficient than algorithms with smaller orders.

4. Suppose that when run with an input of size n, algorithm A requires $2n^2$ operations and algorithm B requires $80n^{3/2}$ operations.
   a. What are orders for algorithms A and B from among the set of power functions?
   b. For what values of n is algorithm A more efficient than algorithm B?
   c. For what values of n is algorithm B at least 100 times more efficient than algorithm A?
5. Suppose that when run with an input of size n, algorithm A requires $10^6 n^2$ operations and algorithm B requires n^3 operations.
   a. What are orders for algorithms A and B from among the set of power functions?
   b. For what values of n is algorithm A more efficient than algorithm B?
   c. For what values of n is algorithm B at least 100 times more efficient than algorithm A?

For each of the algorithm segments in 6–19, assume that n is a positive integer. (a) Compute the actual number of elementary operations (additions, subtractions, multiplications, divisions, and comparisons) that are performed

when the algorithm segment is executed. For simplicity, however, count only comparisons that occur within **if-then** statements; ignore those implied by **for-next** loops. (b) Use the theorem on polynomial orders to find an order for the algorithm segment.

6.
```
for i := 3 to n − 1
    a := 3·n + 2·i − 1
next i
```

7.
```
max := a[1]
for i := 2 to n
    if max < a[i] then max := a[i]
next i
```

8.
```
a := 0
for i := 1 to ⌊n/2⌋
    a := a + 3
next i
```

9.
```
s := 0
for i := 1 to n
    for j := 1 to 2n
        s := s + i·j
    next j
next i
```

10.
```
for k := 2 to n
    for j := 1 to 3n
        x := a[k] − b[j]
    next j
next k
```

11.
```
for k := 1 to n − 1
    for j := 1 to k + 1
        x := a[k] + b[j]
    next j
next k
```

12.
```
for k := 1 to n − 1
    max := a[k]
    for i := k + 1 to n
        if max < a[i] then max := a[i]
    next i
a[k] := max
next k
```

13.
```
for i := 1 to n − 1
    for j := i to n
        if a[ j ] > a[i] then do
            temp := a[i]
            a[i] := a[j]
            a[j] := temp
            end do
    next j
next i
```

14.
```
t := 0
for i := 1 to n
    s := 0
    for j := 1 to i
        s := s + a[j]
    next j
    t := t + s^2
next i
```

15.
```
for i := 1 to n − 1
    p := 1
    q := 1
    for j := i + 1 to n
        p := p·c[j]
        q := q·(c[j])^2
    next j
    r := p + q
next i
```

16.
```
for i: = 1 to n
    s := 0
    for j := 1 to i − 1
        s := s + j·(i − j + 1)
    next j
      r := s^2
next i
```

17.
```
for i := 1 to n
    for j := 1 to ⌊(i+1)/2⌋
        a := (n − i)·(n − j)
     next j
next i
```

18.
```
for i := 1 to n
    for j := ⌊(i + 1)/2⌋ to n
        x := i·j
    next j
next i
```

***H** 19.**
```
for i := 1 to n
    for j := 1 to i
      for k := 1 to j
          x := i·j·k
      next k
    next j
next i
```

20. Construct a table showing the result of each step when insertion sort is applied to the array $a[1] = 6$, $a[2] = 2$, $a[3] = 1$, $a[4] = 8$, and $a[5] = 4$.

21. Construct a table showing the result of each step when insertion sort is applied to the array $a[1] = 7$, $a[2] = 3$, $a[3] = 6$, $a[4] = 9$, and $a[5] = 5$.

22. Construct a trace table showing the action of insertion sort on the array of exercise 20.

23. Construct a trace table showing the action of insertion sort on the array of exercise 21.

24. How many comparisons between values of $a[j]$ and x actually occur when insertion sort is applied to the array of exercise 20?

25. How many comparisons between values of $a[j]$ and x actually occur when insertion sort is applied to the array of exercise 21?

26. According to Example 11.3.6, the maximum number of comparisons needed to perform insertion sort on an array of length five is $5^2 + 5 - 2 = 28$. Find an array of length five that requires the maximum number of comparisons when insertion sort is applied to it.

***H* 27.** Consider the recurrence relation that arose in Example 11.3.7: $E_1 = 0$ and $E_k = E_{k-1} + \frac{k+1}{2}$, for each integer $k \geq 2$.

a. Use iteration to find an explicit formula for the sequence.

b. Use mathematical induction to verify the correctness of the formula.

Exercises 28–35 refer to *selection sort*, which is another algorithm to arrange the items in an array in ascending order.

Algorithm 11.3.2 Selection Sort

[Given an array a[1], a[2], a[3], …, a[n], this algorithm selects the smallest element and places it in the first position, then selects the second smallest element and places it in the second position, and so forth, until the entire array is sorted. In general, for each k = 1 to n − 1, the kth step of the algorithm selects the index of the array item with minimum value from among a[k + 1], a[k + 2], a[k + 3], . . . , a[n]. Once this index is found, the value of the corresponding array item is interchanged with the value of a[k] unless the index already equals k. At the end of execution the array elements are in order.]

Input: *n [a positive integer], a[1], a[2], a[3], . . . , a[n] [an array of data items capable of being ordered]*

Algorithm Body:

```
for k := 1 to n − 1
    IndexOfMin := k
    for i := k + 1 to n
        if (a[i] < a[IndexOfMin])
        then IndexOfMin := i
    next i
    if IndexOfMin ≠ k then
        Temp := a[k]
        a[k] := a[IndexOfMin]
        a[IndexOfMin] := Temp
next k
```

Output: *a*[1], *a*[2], *a*[3], . . . , *a*[*n*] *[in ascending order]*

The action of selection sort can be represented pictorially as follows:

$$a[1]\ a[2] \cdots \boxed{a[k]}\, a[k+1] \cdots a[n]$$

$\uparrow$

*k*th step: Find the index of the array element with minimum value from among $a[k + 1], \ldots, a[n]$. If the value of this array element is less than the value of $a[k]$, then its value and the value of $a[k]$ are interchanged.

28. Construct a table showing the interchanges that occur when selection sort is applied to the array $a[1] = 7$, $a[2] = 3$, $a[3] = 8$, $a[4] = 4$, and $a[5] = 2$.

29. Construct a table showing the interchanges that occur when selection sort is applied to the array $a[1] = 6$, $a[2] = 4$, $a[3] = 5$, $a[4] = 8$, and $a[5] = 1$.

30. Construct a trace table showing the action of selection sort on the array of exercise 28.

31. Construct a trace table showing the action of selection sort on the array of exercise 29.

32. When selection sort is applied to the array of exercise 28, how many times is the comparison in the **if-then** statement performed?

33. When selection sort is applied to the array of exercise 29, how many times is the comparison in the **if-then** statement performed?

34. When selection sort is applied to an array $a[1]$, $a[2]$, $a[3]$, $a[4]$, how many times is the comparison in the **if-then** statement performed?

35. Consider applying selection sort to an array $a[1]$, $a[2]$, $a[3]$, . . . , $a[n]$.

a. How many times is the comparison in the **if-then** statement performed when $a[1]$ is compared to each of $a[2]$, $a[3]$, . . . , $a[n]$?

b. How many times is the comparison in the **if-then** statement performed when $a[2]$ is compared to each of $a[3]$, $a[4]$, . . . , $a[n]$?

c. How many times is the comparison in the **if-then** statement performed when $a[k]$ is compared to each of $a[k-1], a[k+2], \ldots, a[n]$?

***H* d.** Using the number of times the comparison in the **if-then** statement is performed as a measure of the time efficiency of selection sort, find a worst-case order for selection sort. Use the theorem on polynomial orders.

Exercises 36–39 refer to the following algorithm to compute the value of a real polynomial.

Algorithm 11.3.3 Term-by-Term Polynomial Evaluation

[This algorithm computes the value of a polynomial $a[n]x^n + a[n-1]x^{n-1} + \cdots + a[2]x^2 + a[1]x + a[0]$ *by computing each term separately, starting with* $a[0]$*, and adding it to an accumulating sum.]*

Input: *n [a nonnegative integer],* $a[0], a[1], a[2], \ldots, a[n]$ *[an array of real numbers], x [a real number]*

Algorithm Body:

```
polyval := a[0]
for i := 1 to n
    term := a[i]
    for j := 1 to i
        term := term·x
    next j
    polyval := polyval + term
next i
[At this point
polyval = a[n]x^n + a[n-1]x^(n-1)
                  + ··· + a[2]x^2 + a[1]x + a[0].]
```

Output: *polyval [a real number]*

36. Trace Algorithm 11.3.3 for the input $n = 3$, $a[0] = 2, a[1] = 1, a[2] = -1, a[3] = 3$, and $x = 2$.

37. Trace Algorithm 11.3.3 for the input $n = 2$, $a[0] = 5, a[1] = -1, a[2] = 2$, and $x = 3$.

38. Let s_n = the number of additions and multiplications that are performed when Algorithm 11.3.3 is executed for a polynomial of degree n. Express s_n as a function of n.

39. Use the theorem on polynomial orders to find an order for Algorithm 11.3.3.

Exercises 40–43 refer to another algorithm, known as Horner's rule, for finding the value of a polynomial.

Algorithm 11.3.4 Horner's Rule

[This algorithm computes the value of a polynomial $a[n]x^n + a[n-1]x^{n-1} + \cdots + a[2]x^2 + a[1]x + a[0]$ *by nesting successive additions and multiplications as indicated in the following parenthesization:*

$$((\cdots((a[n]x + a[n-1])x + a[n-2])x + \cdots + a[2])x + a[1])x + a[0].$$

At each stage, starting with $a[n]$*, the current value of polyval is multiplied by x and the next lower coefficient of the polynomial is added to it.]*

Input: *n [a nonnegative integer],* $a[0], a[1], a[2], \ldots, a[n]$ *[an array of real numbers], x [a real number]*

Algorithm Body:

```
polyval := a[n]
for i := 1 to n
    polyval := polyval·x + a[n - i]
next i
[At this point
polyval = a[n]x^n + a[n-1]x^(n-1)
                  + ··· + a[2]x^2 + a[1]x + a[0].]
```

Output: *polyval [a real number]*

40. Trace Algorithm 11.3.4 for the input $n = 3$, $a[0] = 2$, $a[1] = 1$, $a[2] = -1$, $a[3] = 3$, and $x = 2$.

41. Trace Algorithm 11.3.4 for the input $n = 2$, $a[0] = 5$, $a[1] = -1$, $a[2] = 2$, and $x = 3$.

***H* 42.** Let t_n = the number of additions and multiplications that are performed when Algorithm 11.3.4 is executed for a polynomial of degree n. Express t_n as a function of n.

43. Use the theorem on polynomial orders to find an order for Algorithm 11.3.4. How does this order compare with that of Algorithm 11.3.3?

ANSWERS FOR TEST YOURSELF

1. one iteration of the innermost loop **2.** n **3.** n^2; n^2

11.4 Exponential and Logarithmic Functions: Graphs and Orders

Although this may seem a paradox, all exact science is dominated by the idea of approximation. —Bertrand Russell, 1872–1970

Exponential and logarithmic functions are of great importance in mathematics in general and in computer science in particular. Several important computer algorithms have execution times that involve logarithmic functions of the size of the input data (which means they are relatively efficient for large data sets), and some have execution times that are exponential functions of the size of the input data (which means they are extremely inefficient for large data sets). In addition, since exponential and logarithmic functions arise naturally in the descriptions of many growth and decay processes and in the computation of many kinds of probabilities, these functions are used in the analysis of computer operating systems, in queuing theory, and in the theory of information.

Graphs of Exponential Functions

As defined in Section 7.2, the exponential function with base $b > 0$ is the function that sends each real number x to b^x. The graph of the exponential function with base 2 (together with a partial table of its values) is shown in Figure 11.4.1. Note that the values of this function increase with extraordinary rapidity. If we tried to continue drawing the graph using the scale shown in Figure 11.4.1, we would have to plot the point $(10, 2^{10})$ more than 21 feet above the horizontal axis. And the point $(30, 2^{30})$ would be located more than 610,080 miles higher—well beyond the moon!

x	2^x
0	$2^0 = 1$
1	$2^1 = 2$
2	$2^2 = 4$
3	$2^3 = 8$
–1	$2^{-1} = 0.5$
–2	$2^{-2} = 0.25$
–3	$2^{-3} = 0.125$
0.5	$2^{0.5} \cong 1.414$
–0.5	$2^{-0.5} \cong 0.707$

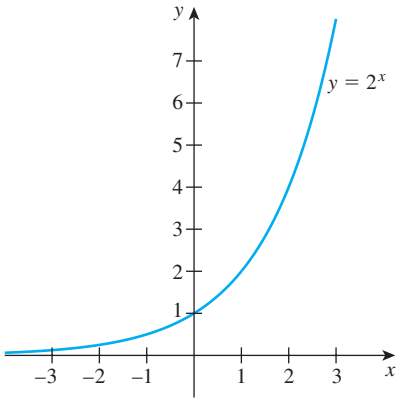
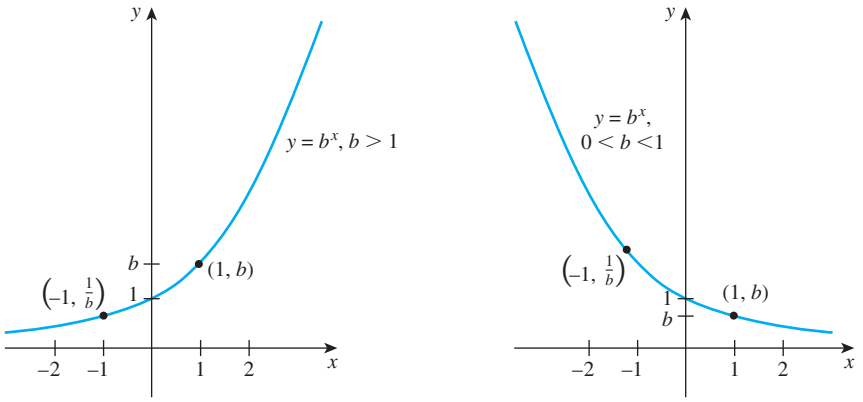


FIGURE 11.4.1 The Exponential Function with Base 2

The graph of any exponential function with base $b > 1$ has a shape that is similar to the graph of the exponential function with base 2. If $0 < b < 1$, then $1/b > 0$ and the graph of the exponential function with base b is the reflection across the vertical axis of the exponential function with base $1/b$. These facts are illustrated in Figure 11.4.2.



Graph of the exponential function with base $b > 1$

(a)

Graph of the exponential function with base b where $0 < b < 1$

(b)

FIGURE 11.4.2 Graphs of Exponential Functions

Bettmann/Getty Images

John Napier (1550–1617)

Graphs of Logarithmic Functions

Logarithms were first introduced by the Scotsman John Napier. Astronomers and navigators found them so useful for reducing the time needed to do multiplication and division that they quickly gained wide acceptance and played a crucial role in the remarkable development of those areas in the seventeenth century. Nowadays, however, electronic calculators and computers are available to handle most computations quickly and conveniently, and logarithms and logarithmic functions are used primarily as conceptual tools.

Recall the definition of the logarithmic function with base b from Section 7.1. We state it formally below.

Definition

If b is a positive real number not equal to 1, then the **logarithmic function with base b, $\log_b$: $\mathbf{R}^+ \to \mathbf{R}$**, is the function that sends each positive real number x to the number $\log_b x$, which is the exponent to which b must be raised to obtain x.

The logarithmic function with base b is, in fact, the inverse of the exponential function with base b. (See exercise 10 at the end of this section.) It follows that the graphs of the two functions are symmetric with respect to the line $y = x$. The graph of the logarithmic function with base $b > 1$ is shown in Figure 11.4.3 on the next page.

If its base b is greater than 1, the logarithmic function is increasing. Analytically, this means that

if $b > 1$, then for all positive numbers x_1 and x_2,

$$\text{if } x_1 < x_2, \text{ then } \log_b(x_1) < \log_b(x_2). \qquad 11.4.1$$

Note As examples, $\log_2(1{,}024)$ is only 10 and $\log_2(1{,}048{,}576)$ is just 20.

Corresponding to the rapid growth of the exponential function, however, is the very slow growth of the logarithmic function. Thus you must go very far out on the horizontal axis to find points whose logarithms are large numbers.

The following example shows how to make use of the increasing nature of the logarithmic function with base 2 to derive a remarkably useful property.

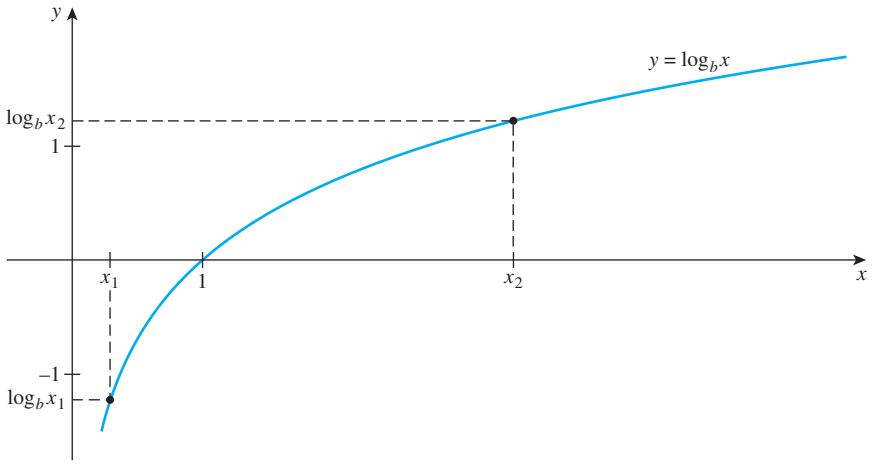


FIGURE 11.4.3 The Graph of the Logarithmic Function with Base $b > 1$

Example 11.4.1 **Base 2 Logarithms of Numbers between Two Consecutive Powers of 2**

Prove the following property:

a. If k is an integer and x is a real number with

$$2^k \le x < 2^{k+1}, \text{ then } \lfloor \log_2 x \rfloor = k. \qquad 11.4.2$$

b. Describe property (11.4.2) in words and give a graphical interpretation of the property for $x > 1$.

Solution

a. Suppose that k is an integer and x is a real number with

$$2^k \le x < 2^{k+1}.$$

Because the logarithmic function with base 2 is increasing, this implies that

$$\log_2(2^k) \le \log_2 x < \log_2(2^{k+1}).$$

But $\log_2(2^k) = k$ *[the exponent to which you must raise* 2 *to get* 2^k *is k]* and $\log_2(2^{k+1}) = k + 1$ *[for a similar reason].* Hence

$$k \le \log_2 x < k + 1.$$

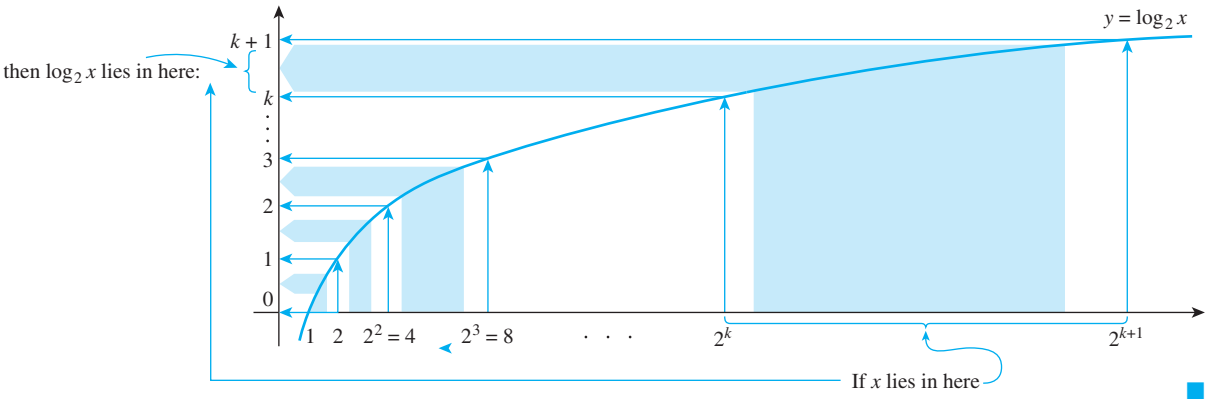
By definition of the floor function, then

$$\lfloor \log_2 x \rfloor = k.$$

b. Recall that the floor of a positive number is its integer part. For instance, $\lfloor 2.82 \rfloor = 2$. Hence property (11.4.2) can be described in words as follows:

> If x is a positive number that lies between two consecutive integer powers of 2, the floor of the logarithm with base 2 of x is the exponent of the smaller power of 2.

A graphical interpretation follows:



One consequence of property (11.4.2) does not appear particularly interesting in its own right but is frequently needed as a step in the analysis of algorithm efficiency.

Example 11.4.2 **When $\lfloor \log_2(n-1) \rfloor = \lfloor \log_2 n \rfloor$**

Prove the following property:

For any odd integer $n > 1$, $\lfloor \log_2(n-1) \rfloor = \lfloor \log_2 n \rfloor$. 11.4.3

Solution If n is an odd integer that is greater than 1, then n lies strictly between two successive powers of 2:

$$2^k < n < 2^{k+1} \quad \text{for some integer } k > 0. \tag{11.4.4}$$

It follows that $2^k \leq n-1$ because $2^k < n$ and both 2^k and n are integers. Consequently,

$$2^k \leq n-1 < 2^{k+1}. \tag{11.4.5}$$

Applying property (11.4.2) to both inequalities (11.4.4) and (11.4.5) gives

$$\lfloor \log_2 n \rfloor = k \text{ and also } \lfloor \log_2(n-1) \rfloor = k.$$

Hence $\lfloor \log_2 n \rfloor = \lfloor \log_2(n-1) \rfloor$. ■

Application: Number of Bits Needed to Represent an Integer in Binary Notation

Given a positive integer n, how many binary digits are needed to represent n? To answer this question, recall from Section 5.4 that any positive integer n can be written in a unique way as

$$n = 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where k is a nonnegative integer and each $c_0, c_1, c_2, \ldots c_{k-1}$ is either 0 or 1. Then the binary representation of n is

$$1 c_{k-1} c_{k-2} \cdots c_2 c_1 c_0,$$

and so the number of binary digits needed to represent n is $k+1$.

What is $k+1$ as a function of n? Observe that since each $c_i \leq 1$,

$$n = 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0 \leq 2^k + 2^{k-1} + \cdots + 2^2 + 2 + 1.$$

Now, by the formula for the sum of a geometric sequence (Theorem 5.2.2),

$$2^k + 2^{k-1} + \cdots + 2^2 + 2 + 1 = \frac{2^{k+1} - 1}{2 - 1} = 2^{k+1} - 1.$$

Hence, by transitivity of order,

$$n \le 2^{k+1} - 1 < 2^{k+1}. \qquad 11.4.6$$

In addition, because each $c_i \ge 0$,

$$2^k \le 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0 = n. \qquad 11.4.7$$

Putting inequalities (11.4.6) and (11.4.7) together gives the double inequality

$$2^k \le n < 2^{k+1}.$$

Then, by property (11.4.2),

$$k = \lfloor \log_2 n \rfloor,$$

and so the number of binary digits needed to represent n is $\lfloor \log_2 n \rfloor + 1$.

Example 11.4.3 **Number of Bits in a Binary Representation**

How many binary digits are needed to represent 52,837 in binary notation?

Solution If you compute the logarithm with base 2 using the formula in part (a) of Theorem 7.2.1 and a calculator or computer that gives you approximate values of logarithms with base 10, you find that

$$\log_2(52{,}837) \cong \frac{\log_{10}(52{,}837)}{\log_{10}(2)} \cong \frac{4.722938151}{0.3010299957} \cong 15.7.$$

Thus the binary representation of 52,837 has $\lfloor 15.7 \rfloor + 1 = 15 + 1 = 16$ binary digits. ■

Application: Using Logarithms to Solve Recurrence Relations

In Chapter 5 we discussed methods for solving recurrence relations. A class of recurrence relations that is very important in computer science has solutions that can be expressed in terms of logarithms. One such recurrence relation is discussed in the next example.

Example 11.4.4 **A Recurrence Relation with a Logarithmic Solution**

Define a sequence $a_1, a_2, a_3, \ldots$ recursively as follows:

$$a_1 = 1$$
$$a_k = 2a_{\lfloor k/2 \rfloor} \quad \text{for each integer } k \ge 2.$$

a. Use iteration to guess an explicit formula for this sequence.

b. Use strong mathematical induction to confirm the correctness of the formula obtained in part (a).

Solution

a. Begin by iterating to find the values of the first few terms of the sequence.

$$\begin{aligned}
a_1 &= 1 && 1 = 2^0\\
a_2 &= 2a_{\lfloor 2/2\rfloor} = 2a_1 = 2\cdot 1 = 2 \\
a_3 &= 2a_{\lfloor 3/2\rfloor} = 2a_1 = 2\cdot 1 = 2 && 2 = 2^1\\
a_4 &= 2a_{\lfloor 4/2\rfloor} = 2a_2 = 2\cdot 2 = 4 \\
a_5 &= 2a_{\lfloor 5/2\rfloor} = 2a_2 = 2\cdot 2 = 4 \\
a_6 &= 2a_{\lfloor 6/2\rfloor} = 2a_3 = 2\cdot 2 = 4 \\
a_7 &= 2a_{\lfloor 7/2\rfloor} = 2a_3 = 2\cdot 2 = 4 && 4 = 2^2\\
a_8 &= 2a_{\lfloor 8/2\rfloor} = 2a_4 = 2\cdot 4 = 8 \\
a_9 &= 2a_{\lfloor 9/2\rfloor} = 2a_4 = 2\cdot 4 = 8 \\
&\vdots \qquad\qquad \vdots \\
a_{15} &= 2a_{\lfloor 15/2\rfloor} = 2a_7 = 2\cdot 4 = 8 && 8 = 2^3\\
a_{16} &= 2a_{\lfloor 16/2\rfloor} = 2a_8 = 2\cdot 8 = 16 && 16 = 2^4\\
&\vdots \qquad\qquad \vdots
\end{aligned}$$

Note that in each case when the subscript n is between two powers of 2, a_n equals the smaller power of 2. More precisely:

$$\text{If } 2^i \le n < 2^{i+1}, \text{ then } a_n = 2^i. \qquad 11.4.8$$

Now since n satisfies the inequality

$$2^i \le n < 2^{i+1},$$

then (by property 11.4.2)

$$i = \lfloor \log_2 n \rfloor.$$

Substituting into statement (11.4.8) suggests that

$$a_n = 2^{\lfloor \log_2 n \rfloor}.$$

b. The following proof shows that the recursively defined sequence defined in this example does in fact satisfy the formula obtained in part (a). In other words, if a_1, a_2, a_3, . . . is a sequence of numbers that satisfies

$$a_1 = 1, \quad \text{and} \quad a_k = 2a_{\lfloor k/2\rfloor} \quad \text{for each integer } k \ge 2,$$

then the sequence satisfies the formula

$$a_n = 2^{\lfloor \log_2 n \rfloor} \quad \text{for every integer } n \ge 1.$$

Proof:

Let $a_1, a_2, a_3, \ldots$ be the sequence defined by specifying that $a_1 = 1$ and $a_k = 2a_{\lfloor k/2\rfloor}$ for each integer $k \ge 2$, and let the property $P(n)$ be the equation

$$a_n = 2^{\lfloor \log_2 n \rfloor}. \quad \leftarrow P(n)$$

We will use strong mathematical induction to prove that for every integer $n \ge 1$, $P(n)$ is true.

Show that P(1) is true: By definition of $a_1, a_2, a_3, \ldots$, we have that $a_1 = 1$. Now it is also the case that $2^{\lfloor \log_2 1 \rfloor} = 2^0 = 1$. Thus $a_1 = 2^{\lfloor \log_2 1 \rfloor}$ and $P(1)$ is true.

Show that for every integer $k \geq 1$, if P(i) is true for each integer i from 1 through k, then P(k +1) is also true: Let k be any integer with $k \geq 1$, and suppose that

$$a_i = 2^{\lfloor \log_2 i \rfloor} \text{ for each integer } i \text{ with } 1 \leq i \leq k. \qquad \leftarrow \text{inductive hypothesis}$$

We must show that

$$a_{k+1} = 2^{\lfloor \log_2 (k+1) \rfloor}. \qquad \leftarrow P(k+1)$$

Consider the two cases: k is even and k is odd.

Case 1 (k is even): In this case, $k + 1$ is odd, and

$$\begin{aligned}
a_{k+1} &= 2a_{\lfloor (k+1)/2 \rfloor} && \text{by definition of } a_1, a_2, a_3, \ldots \\
&= 2a_{k/2} && \text{because } \lfloor (k+1)/2 \rfloor = k/2 \text{ since } k+1 \text{ is odd} \\
&= 2 \cdot 2^{\lfloor \log_2 (k/2) \rfloor} && \text{by inductive hypothesis because, since } k \text{ is even, } k \geq 2, \text{ and so } k/2 \geq 1 \\
&= 2^{\lfloor \log_2 (k/2) \rfloor + 1} && \text{by the laws of exponents from algebra (7.2.1)} \\
&= 2^{\lfloor \log_2 k - \log_2 2) \rfloor + 1} && \text{by the identity } \log_b (x/y) = \log_b x - \log_b y \text{ from Theorem 7.2.1} \\
&= 2^{\lfloor \log_2 k - 1 \rfloor + 1} && \text{since } \log_2 2 = 1 \\
&= 2^{\lfloor \log_2 k \rfloor - 1 + 1} && \text{by substituting } x = \log_2 k \text{ into the identity} \\
&= 2^{\lfloor \log_2 k \rfloor} && \lfloor x - 1 \rfloor = \lfloor x \rfloor - 1 \text{ derived in exercise 15 of Section 4.6} \\
&= 2^{\lfloor \log_2 (k+1) \rfloor} && \text{by property (11.4.3).}
\end{aligned}$$

Case 2 (k is odd): The analysis of this case is very similar to that of case 1 and is left as exercise 51 at the end of the section.

Thus in either case, $a_n = 2^{\lfloor \log_2 (k+1) \rfloor}$, as was to be shown. ■

Exponential and Logarithmic Orders

Now consider the question "How do graphs of logarithmic and exponential functions compare with graphs of power functions?" It turns out that for large enough values of x, the graph of the logarithmic function with any base $b > 1$ lies *below* the graph of every power function with a positive exponent, and the graph of the exponential function with any base $b > 1$ lies *above* the graph of each of these power functions. In analytic terms, this says the following:

For all real numbers b and r with $b > 1$ and $r > 0$, there is a positive real number s such that

$$\log_b x \leq x^r \quad \text{for every real number } x \geq s. \qquad 11.4.9$$

and

$$x^r \leq b^x \quad \text{for every real number } x \geq s. \qquad 11.4.10$$

These statements have the following implications for O-notation.

For all real numbers b and r with $b > 1$ and $r > 0$,

$$\log_b n \text{ is } O(n^r) \qquad 11.4.11$$

and

$$n^r \text{ is } O(b^n) \qquad 11.4.12$$

Another important function in the analysis of algorithms is the function f defined by the formula

$$f(x) = x \log_b x \quad \text{for every real number } x > 0.$$

For large values of x, the graph of this function fits in between the graph of the identity function and the graph of the squaring function. More precisely:

For every real number b with $b > 1$, there is a positive real number s such that for every real number $x \geq s$,

$$x \leq x \log_b x \leq x^2. \qquad 11.4.13$$

The O-notation versions of these facts are as follows:

For every real number $b > 1$,

$$n \text{ is } O(n \log_b n) \text{ and } n \log_b n \text{ is } O(n^2). \qquad 11.4.14$$

Although proofs of some of these facts require calculus, some cases can be verified using the algebra of inequalities. (See the exercises at the end of this section.) Figure 11.4.4 illustrates the relationships among some power functions, the logarithmic function with base 2, the exponential function with base 2, and the function defined by the formula $x \longrightarrow x \log_2 x$. Note that different scales are used on the horizontal and vertical axes.

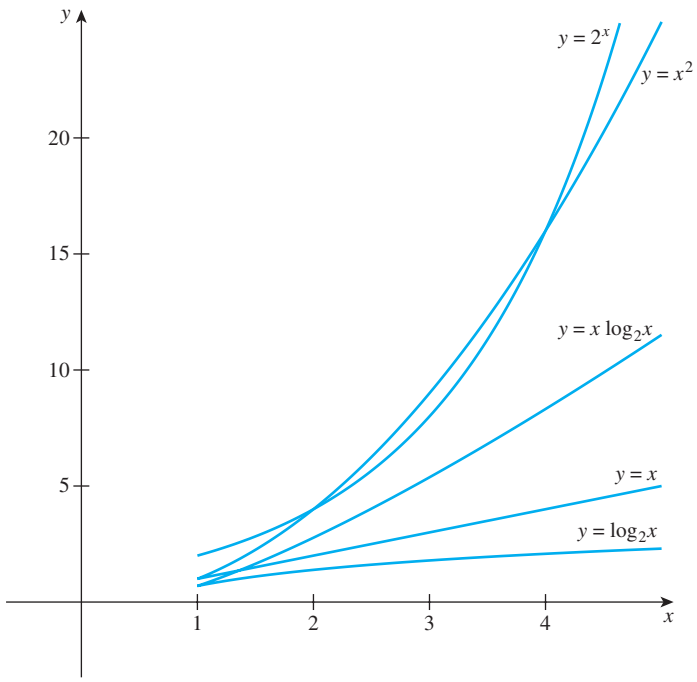


FIGURE 11.4.4 Graphs of Some Logarithmic, Exponential, and Power Functions

Examples 11.4.5 and 11.4.6 use properties of logarithms together with theorems from Section 11.2 to derive orders for combinations that involve logarithmic and exponential functions.

Example 11.4.5 **Orders That Involve Logarithmic Functions**

a. Show that if b and c are any real numbers with $b > 1$ and $c > 1$, then $\log_b n$ and $\log_c n$ have the same order.

b. Show that $n + n \log_2 n$ is $\Theta(n \log_2 n)$.

Solution

a. By part (d) of Theorem 7.2.1,

$$\log_b n = \frac{\log_c n}{\log_c b} = \left(\frac{1}{\log_c b}\right)\log_c n.$$

Since both $b > 1$ and $c > 1$, then $\log_c b > 0$, and so $\dfrac{1}{\log_c b} > 0$. Thus, by Theorem 11.2.8(c),

$$\left(\frac{1}{\log_c b}\right)\log_c n \text{ is } \Theta(\log_c n), \text{ and so } \log_b n \text{ is } \Theta(\log_c n).$$

Exactly the same reasoning with b and c interchanged gives that

$$\log_c n \quad \text{is} \quad \Theta(\log_b n).$$

Thus $\log_b n$ and $\log_c n$ have the same order.

b. By Theorem 11.2.7, n is $\Theta(n)$ and $n \log_2 n$ is $\Theta(n \log_2 n)$. In addition, by property 11.4.13, there is a positive real number r such that for every integer $n \geq r$, $n \leq n \log_2 n$. Thus it follows from Theorem 11.2.9(c) that $n + n \log_2 n$ is $\Theta(n \log_2 n)$. ■

Example 11.4.6 **An Exponential Order**

Show that $n!$ is $O(n^n)$.

Solution

For any positive integer n,

$$n! = \underbrace{n \cdot (n-1) \cdot (n-2) \cdot 2 \cdot 1}_{n \text{ factors}}$$
$$\leq \underbrace{n \cdot n \cdot n \cdot n \cdot n}_{n \text{ factors}} = n^n$$

because $(n-1) \leq n$, $(n-2) \leq n, \ldots, 2 \leq n$, and $1 \leq n$. Let $B = 1$ and $b = 1$. Then, since $n! \geq 0$ when $n \geq b$,

$$0 \leq n! \leq n^n \quad \text{for every integer } n \geq b.$$

Thus $n!$ is $O(n^n)$ by definition of O-notation. ■

Example 11.4.7 shows how a logarithmic order can arise from the computation of a certain kind of sum. It requires the following fact from calculus:

The area underneath the graph of $y = 1/x$ between $x = 1$ and $x = n$ equals $\ln n$, where $\ln n = \log_e n$. This fact is illustrated in Figure 11.4.5.

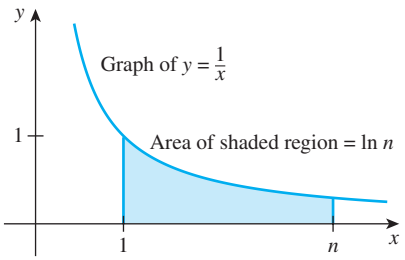


FIGURE 11.4.5 Area under graph of $y = \dfrac{1}{x}$ between $x = 1$ and $x = n$

Example 11.4.7 **Order of a Harmonic Sum**

Sums of the form $1+\frac{1}{2}+\cdots+\frac{1}{n}$ are called *harmonic sums*. They occur in the analysis of various computer algorithms such as quick sort. Show that $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ is $\Omega(\ln n)$ by performing the steps shown below:

a. Interpret Figure 11.4.6 to show that

$$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \leq \ln n.$$

and

$$\ln n \leq 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}.$$

b. Show that if n is an integer that is at least 3, then $1 \leq \ln n$.

c. Deduce from (a) and (b) that if the integer n is greater than or equal to 3, then

$$\ln n \leq 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \leq 2 \ln n.$$

d. Deduce from (c) that

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \text{ is } \Theta(\ln n).$$

Solution

a. Figure 11.4.6(a) shows rectangles whose bases are the intervals between each pair of integers from 1 to n and whose heights are the heights of the graph of $y = 1/x$ above the right-hand endpoints of the intervals. Figure 11.4.6(b) shows rectangles with the same bases but whose heights are the heights of the graph above the left-hand endpoints of the intervals.

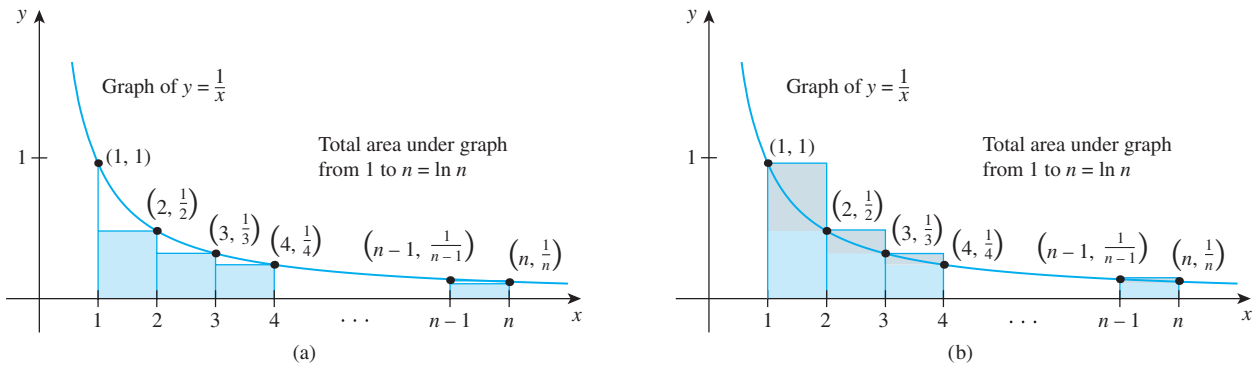


FIGURE 11.4.6

Now the area of each rectangle is its base times its height. Since all the rectangles have base 1, the area of each rectangle equals its height. Thus in Figure 11.4.6(a),

$$\text{the area of the rectangle from 1 to 2 is } \frac{1}{2};$$
$$\text{the area of the rectangle from 2 to 3 is } \frac{1}{3};$$
$$\vdots$$
$$\text{the area of the rectangle from } n-1 \text{ to } n \text{ is } \frac{1}{n}.$$

So the sum of the areas of all the rectangles is $\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$. From the picture it is clear that this sum is less than the area underneath the graph of f between $x = 1$ and $x = n$, which is known to equal $\ln n$. Hence

$$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \le \ln n.$$

A similar analysis of the areas of the combined blue and gray rectangles in Figure 11.4.6(b) shows that

$$\ln n \le 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}.$$

b. Suppose n is an integer and $n \ge 3$. Since $e \cong 2.718$, then $n \ge e$. Now the logarithmic function with base e is strictly increasing. Thus since $e \le n$, then $1 = \ln e \le \ln n$.

c. By part (a),

$$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \le \ln n,$$

and by part (b),

$$1 \le \ln n.$$

Adding these two inequalities together gives

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \le 2 \ln n \quad \text{for each integer } n \ge 3.$$

d. Combining the results of parts (a) and (c) leads to the conclusion that for every integer $n \ge 3$,

$$\ln n \le 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \le 2 \ln n.$$

Let $A = 1$, $B = 2$, and $k = 3$. Then $\ln n > 0$ for $n \ge 3$ and

$$A \ln n \le 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \le B \ln n \quad \text{for every integer } n > k.$$

Hence by definition of Θ-notation,

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \text{ is } \Theta(\ln n).$$ ■

Now by Example 11.4.5(a), all logarithmic functions have the same order, and thus for each real number $b > 1$,

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \text{ is } \Theta(\log_b n).$$

TEST YOURSELF

1. The domain of any exponential function is _____, and its range is _____.
2. The domain of any logarithmic function is _____, and its range is _____.
3. If k is an integer and $2^k \le x < 2^{k+1}$, then $\lfloor \log_2 x \rfloor =$ _____.
4. If b is a real number with $b > 1$, then there is a positive real number s with the property that for any real number x that is greater than s, when the quantities x, x^2, $\log x$, and $x \log x$ are arranged in order of increasing size, the result is _____.
5. If n is a positive integer, then $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ has order _____.

EXERCISE SET 11.4

Graph each function defined in 1–8.

1. $f(x) = 3^x$ for each real number x
2. $g(x) = \left(\frac{1}{3}\right)^x$ for each real number x
3. $h(x) = \log_{10} x$ for each positive real number x
4. $k(x) = \log_2 x$ for each positive real number x
5. $F(x) = \lfloor \log_2 x \rfloor$ for each positive real number x
6. $G(x) = \lfloor \log_2 x \rfloor$ for each positive real number x
7. $H(x) = x \log_2 x$ for each positive real number x
8. $K(x) = x \log_{10} x$ for each positive real number x
9. The scale of the graph shown in Figure 11.4.1 is one-fourth inch to each unit. If the point $(2, 2^{64})$ is plotted on the graph of $y = 2^x$, how many miles will it lie above the horizontal axis? What is the ratio of the height of the point to the distance of the earth from the sun? (There are 12 inches per foot and 5,280 feet per mile. The earth is approximately 93,000,000 miles from the sun on average.) ($\frac{1}{4}$ inch $\cong$ 0.635 cm, 1 mile $\cong$ 0.62 km)
10. **a.** Use the definition of logarithm to show that $\log_b b^x = x$ for every real number x.
    b. Use the definition of logarithm to show that $b^{\log_b x} = x$ for every positive real number x.
    c. By the result of exercise 28 in Section 7.3, if $f: X \to Y$ and $g: Y \to X$ are functions and $g \circ f = I_X$ and $f \circ g = I_Y$, then f and g are inverse functions. Use this result to show that $\log_b$ and $\exp_b$ (the exponential function with base b) are inverse functions.
11. Let $b > 1$.
    a. Use the fact that $u = \log_b v \Leftrightarrow v = b^u$ to show that a point (u, v) lies on the graph of the logarithmic function with base b if, and only if, (v, u) lies on the graph of the exponential function with base b.
    b. Plot several pairs of points of the form (u, v) and (v, u) on a coordinate system. Describe the geometric relationship between the locations of the points in each pair.
    c. Draw the graphs of $y = \log_2 x$ and $y = 2^x$. Describe the geometric relationship between these graphs.
12. Give a graphical interpretation for property (11.4.2) in Example 11.4.1(a) for $0 < x < 1$.
13. *H* Suppose a positive real number x satisfies the inequality $10^m \le x < 10^{m+1}$ where m is an integer. What can be inferred about $\lfloor \log_{10} x \rfloor$? Justify your answer.
14. **a.** Prove that if x is a positive real number and k is a nonnegative integer such that $2^{k-1} < x \le 2^k$, then $\lceil \log_2 x \rceil = k$.
    b. Describe in words the statement proved in part (a).
15. If n is an odd integer and $n > 1$, is $\lceil \log_2(n-1) \rceil = \lceil \log_2(n) \rceil$? Justify your answer.
16. *H* If n is an odd integer and $n > 1$, is $\lceil \log_2(n+1) \rceil = \lceil \log_2(n) \rceil$? Justify your answer.
17. If n is an odd integer and $n > 1$, is $\lfloor \log_2(n+1) \rfloor = \lfloor \log_2(n) \rfloor$? Justify your answer.

In 18 and 19, indicate how many binary digits are needed to represent the numbers in binary notation. Use the method shown in Example 11.4.3.

18. 148,206
19. 5,067,329

20. It was shown in the text that the number of binary digits needed to represent a positive integer n is $\lfloor \log_2 n \rfloor + 1$. Can this also be given as $\lceil \log_2 n \rceil$? Why or why not?

In each of 21 and 22, a sequence is specified by a recurrence relation and initial conditions. In each case, (a) use iteration to guess an explicit formula for the sequence; (b) use strong mathematical induction to confirm the correctness of the formula you obtained in part (a).

21. $a_k = a_{\lfloor k/2 \rfloor} + 2$, for each integer $k \geq 2$
$a_1 = 1$

22. $b_k = b_{\lfloor k/2 \rfloor} + 1$, for each integer $k \geq 2$
$b_1 = 1$.

H 23. Define a sequence $c_1, c_2, c_3, \ldots$ recursively as follows:

$$c_1 = 0$$
$$c_k = c_{\lfloor k/2 \rfloor} + k, \quad \text{for each integer } k \geq 2.$$

Use strong mathematical induction to show that $c_n \leq n^2$ for every integer $n \geq 1$.

***H 24.** Use strong mathematical induction to show that for the sequence of exercise 23, $c_n \leq n \log_2 n$, for every integer $n \geq 4$.

Exercises 25 and 26 refer to properties 11.4.9 and 11.4.10. To solve them, think big!

25. Find a real number $x > 3$ such that $\log_2 x < x^{1/10}$.

26. Find a real number $x > 1$ such that $x^{50} < 2^x$.

Use Theorems 11.2.7–11.2.9 and properties 11.4.11, 11.4.12, and 11.4.13 to derive each statement in 27–30.

27. $2n + \log_2 n$ is $\Theta(n)$

28. $n^2 + 5n \log_2 n$ is $\Theta(n^2)$

29. $n^2 + 2^n$ is $\Theta(2^n)$

H 30. 2^{n+1} is $\Theta(2^n)$

H 31. Show that 4^n is not $O(2^n)$.

Prove each of the statements in 32–37, assuming n is an integer variable that takes positive integer values. Use identities from Section 5.2 as needed.

32. $1 + 2 + 2^2 + 2^3 + \cdots + 2^n$ is $\Theta(2^n)$.

H 33. $4 + 4^2 + 4^3 + \cdots + 4^n$ is $\Theta(4^n)$.

34. $2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2n}$ is $\Theta(3^{2n})$.

35. $\dfrac{1}{5} + \dfrac{4}{5^2} + \dfrac{4^2}{5^3} + \cdots + \dfrac{4^n}{5^{n+1}}$ is $\Theta(1)$.

36. $n + \dfrac{n}{2} + \dfrac{n}{4} + \cdots + \dfrac{n}{2^n}$ is $\Theta(n)$.

37. $\dfrac{2n}{3} + \dfrac{2n}{3^2} + \dfrac{2n}{3^3} + \cdots + \dfrac{2n}{3^n}$ is $\Theta(n)$.

38. Quantities of the form

$k_1 n + k_2 n \log n$ for positive integers k_1, k_2, and n

arise in the analysis of the merge sort algorithm in computer science. Show that for any positive integer k,

$$k_1 n + k_2 n \log_2 n \text{ is } \Theta(n \log_2 n).$$

39. Calculate the values of the harmonic sums

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \quad \text{for } n = 2, 3, 4, \text{ and } 5.$$

40. Use part (d) of Example 11.4.7 to show that

$$n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} \text{ is } \Theta(n \ln n).$$

41. Show that $\lfloor \log_2 n \rfloor$ is $\Theta(\log_2 n)$.

42. Show that $\lceil \log_2 n \rceil$ is $\Theta(\log_2 n)$.

43. Prove by mathematical induction that $n \leq 10^n$ for every integer $n \geq 1$.

H 44. Prove by mathematical induction that $\log_2 n \leq n$ for every integer $n \geq 1$.

H 45. Show that if n is a variable that takes positive integer values, then 2^n is $O(n!)$.

46. Let n be a variable that takes positive integer values.

a. Use Example 11.4.6 to show that $\log_2(n!)$ is $O(n \log_2 n)$.

H b. Show that $n^n \leq (n!)^2$ for every integer $n \geq 1$.

c. Use part (b) to show that $\log_2(n!)$ is $\Omega(n \log_2 n)$.

d. Use parts (a) and (c) to find an order for $\log_2(n!)$.

47. For each positive real number u, $\log_2 u < u$. Use this fact and the result of exercise 21 in Section 11.1 to prove the following: For every integer $n \geq 1$, if x is any real number with $x > (2n)^{2n}$, then $\log_2 x < x^{1/n}$.

48. Use the result of exercise 47 above to prove the following: For every integer $n \geq 1$, if x is any real number with $x > (2n)^{2n}$, then $x^n < 2^x$.

Exercises 49 and 50 use L'Hôpital's rule from calculus.

49. a. Let b be any real number greater than 1. Use L'Hôpital's rule and mathematical induction to prove that for every integer $n \geq 1$,

$$\lim_{x \to \infty} \frac{x^a}{b^x} = 0.$$

b. Use the result of part (a) and the definitions of limit and of O-notation to prove that x^n is $O(b^x)$ for any integer $n \geq 1$.

50. a. Let b be any real number greater than 1. Use L'Hôpital's rule to prove that for every integer $n \geq 1$,

$$\lim_{x \to \infty} \frac{\log_b x}{x^{1/n}} = 0.$$

b. Use the result of part (a) and the definitions of limit and of O-notation to prove that $\log_b x$ is $O(x^{1/n})$ for any integer $n \geq 1$.

51. Complete the proof in Example 11.4.4.

ANSWERS FOR TEST YOURSELF

1. the set of all real numbers; the set of all positive real numbers **2.** the set of all positive real numbers; the set of all real numbers **3.** k **4.** $\log_b x < x < x \log_b x < x^2$ **5.** $\ln x$ (or, equivalently, $\log_2 x$)

11.5 Application: Analysis of Algorithm Efficiency II

Hulton Archive/Getty Images

Lady Lovelace
(1815–1852)

In almost every computation a great variety of arrangements for the succession of the processes is possible, and various considerations must influence the selections amongst them for the purposes of a calculating engine. One essential object is to choose that arrangement which shall tend to reduce to a minimum the time necessary for completing the calculation. —Ada Augusta, Countess of Lovelace, 1843

Have you ever played the "guess my number" game? A person thinks of a number between two other numbers—say, 1 and 10 or 1 and 100 for example—and you try to figure out what it is, using the least possible number of guesses. Each time you guess a number, the person tells you whether you are correct, too low, or too high.

If you have played this game, you have probably already hit upon the most efficient strategy: Begin by guessing a number as close to the middle of the two given numbers as possible. If your guess is too high, then the number is between the lower of the two given numbers and the one you first chose. If your guess is too low, then the number is between the number you first chose and the higher of the two given numbers. In either case, you take as your next guess a number as close as possible to the middle of the new range in which you now know the number lies. You repeat this process as many times as necessary until you have found the person's number.

The technique described previously is an example of a general strategy called **divide and conquer**, which works as follows: To solve a problem, reduce it to a fixed number of smaller problems of the same kind, which can themselves be reduced to the same fixed number of smaller problems of the same kind, and so forth until easily resolved problems are obtained. In this case, the problem of finding a particular number in a given range of numbers is reduced at each stage to finding a particular number in a range of numbers approximately half as long.

It turns out that algorithms using a divide-and-conquer strategy are generally quite efficient and nearly always have orders involving logarithmic functions. In this section we define the *binary search* algorithm, which is the formalization of the "guess my number"

game described previously, and we compare the efficiency of binary search to the sequential search discussed in Section 11.3. Then we develop a divide-and-conquer algorithm for sorting, *merge sort*, and compare its efficiency with that of insertion sort and selection sort, which were also discussed in Section 11.3.

Almost a hundred years before the first computer was built and working only from a description of how such a machine might function, Ada Augusta, Countess of Lovelace, foresaw both the general nature of the problems it could address and the importance of designing an efficient arrangement of computations to solve them.

Binary Search

Whereas a sequential search can be performed on an array whose elements are in any order, a binary search can be performed only on an array whose elements are arranged in ascending (or descending) order. Given an array $a[1], a[2], \ldots, a[n]$ of distinct elements arranged in ascending order, consider the problem of trying to find a particular element x in the array.

To use binary search, first compare x to the "middle element" of the array. If the two are equal, the search is successful. If the two are not equal, then because the array elements are in ascending order, comparing the values of x and the middle array element narrows the search either to the lower subarray (consisting of all the array elements below the middle element) or to the upper subarray (consisting of all array elements above the middle element).

The search continues by repeating this basic process over and over on successively smaller subarrays. It terminates either when a match occurs or when the subarray to which the search has been narrowed contains no elements. The efficiency of the algorithm is a result of the fact that at each step, the length of the subarray to be searched is roughly half the length of the array of the previous step. This process is illustrated in Figure 11.5.1.

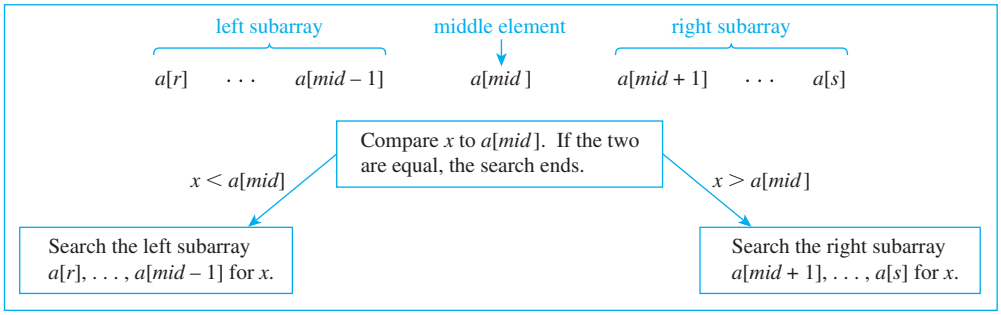


FIGURE 11.5.1 One Iteration of the Binary Search Process

To write down a formal algorithm for binary search, we introduce a variable *index* whose final value will tell us whether or not x is in the array and, if so, will indicate the location of x. Since the array goes from $a[1]$ to $a[n]$, we initialize *index* to be 0. If and when x is found, the value of *index* is changed to the subscript of the array element equaling x. If index still has the value 0 when the algorithm is complete, then x is not one of the elements in the array. Figure 11.5.2 shows the action of a particular binary search.

Formalizing a binary search algorithm also requires that we be more precise about the meaning of the "middle element" of an array. (This issue was side-stepped by careful choice of n in Figure 11.5.2.) If the array consists of an even number of elements, there are

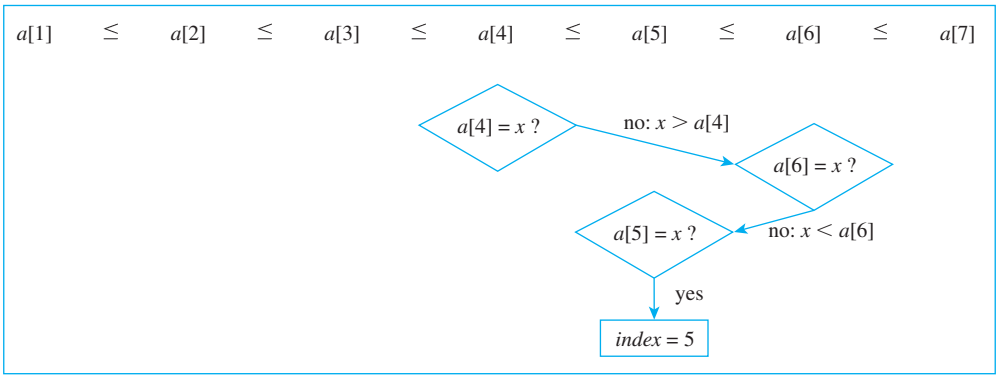


FIGURE 11.5.2 Binary Search of $a[1], a[2], \ldots, a[7]$ for x (for $x = a[5]$)

two elements in the middle. For instance, both $a[6]$ and $a[7]$ are equally in the middle of the following array.

$$\underbrace{a[3] \quad a[4] \quad a[5]}_{\text{three elements}} \quad \underbrace{a[6] \quad a[7]}_{\text{two middle elements}} \quad \underbrace{a[8] \quad a[9] \quad a[10]}_{\text{three elements}}$$

In a case such as this, the algorithm must choose which of the two middle elements to take, the smaller or the larger. The choice is arbitrary—either would do. We will write the algorithm to choose the smaller. The index of the smaller of the two middle elements is the floor of the average of the top and bottom indexes of the array. That is, if

$$\begin{aligned} bot &= \text{the bottom index of the array,} \\ top &= \text{the top index of the array, and} \\ mid &= \text{the lower of the two middle indexes of the array,} \end{aligned}$$

then

$$mid = \left\lfloor \frac{bot + top}{2} \right\rfloor.$$

In this case, $bot = 3$ and $top = 10$, so the index of the "middle element" is

$$mid = \left\lfloor \frac{3 + 10}{2} \right\rfloor = \left\lfloor \frac{13}{2} \right\rfloor = \lfloor 6.5 \rfloor = 6.$$

The following is a formal algorithm for a binary search.

Algorithm 11.5.1 Binary Search

[The aim of this algorithm is to search for an element x in an ascending array of elements a[1], a[2], . . . , a[n]. If x is found, the variable index is set equal to the index of the array element where x is located. If x is not found, index is not changed from its initial value, which is 0. The variables bot and top denote the bottom and top indexes of the array currently being examined.]

Input: *n [a positive integer], a[1], a[2], . . . , a[n] [an array of data items given in ascending order], x [a data item of the same data type as the elements of the array]*

(continued on page 816)

Algorithm Body:

index := 0, *bot* := 1, *top* := *n*

[Compute the middle index of the array, mid. Compare x to a[mid]. If the two are equal, the search is successful. If not, repeat the process either for the lower or for the upper subarray, either giving top the new value mid −1 or giving bot the new value mid +1. Each iteration of the loop either decreases the value of top or increases the value of bot. Thus, if the looping is not stopped by success in the search process, the value of top eventually becomes less than the value of bot, which stops the looping process and shows that x is not an element of the array.]

while (*top* ≥ *bot* and *index* = 0)

$$mid := \left\lfloor \frac{bot + top}{2} \right\rfloor$$

if *a*[*mid*] = *x* **then** *index* := *mid*

if *a*[*mid*] > *x*

then *top* := *mid* − 1

else *bot* := *mid* + 1

end while

[If index has the value 0 at this point, then the **while** *loop was not entered because top < bot, and so x is not in the array. Otherwise, index gives the index of the array where x is located.]*

Output: *index [a nonnegative integer]*

Example 11.5.1 **Tracing the Binary Search Algorithm**

Trace the action of Algorithm 11.5.1 on the variables *index*, *bot*, *top*, *mid*, and the values of *x* given in (a) and (b) below for the input array

a[1] = Ann, *a*[2] = Dawn, *a*[3] = Erik, *a*[4] = Gail, *a*[5] = Juan,
a[6] = Matt, *a*[7] = Max, *a*[8] = Rita, *a*[9] = Tsuji, *a*[10] = Yuen,

where alphabetical ordering is used to compare elements of the array.

a. *x* = Erik b. *x* = Sara

Solution

a.

index	0			3
bot	1		3	
top	10	4		
mid		5	2	3
x	Erik			

b.

index	0			
bot	1	6	9	
top	10			8
mid		5	8	9
x	Sara			

■

The Efficiency of the Binary Search Algorithm

Here briefly is the idea for how to derive the efficiency of the binary search algorithm. At each stage of the binary search process, the length of the new subarray to be searched is

approximately half that of the previous one, and in the worst case, every subarray down to a subarray with a single element must be searched. Consequently, in the worst case, the maximum number of iterations of the algorithm's **while** loop is 1 more than the number of times the original input array can be cut approximately in half. Now if the length n of this array is a power of 2 ($n = 2^k$ for some integer k), then n can be halved exactly $k = \log_2 n = \lfloor \log_2 n \rfloor$ times before an array of length 1 is reached. If n is not a power of 2, then $n = 2^k + m$ for some integer k (where $m < 2^k$), and thus n can be split approximately in half k times also, and so in this case, $k = \lfloor \log_2 n \rfloor$ also. Thus in the worst case, the maximum number of iterations of the **while** loop in the binary search algorithm (which is proportional to the number of comparisons required to execute it) is $\lfloor \log_2 n \rfloor + 1$. The derivation is concluded by noting that $\lfloor \log_2 n \rfloor + 1$ is $O(\log_2 n)$.

The details of the derivation are developed in Examples 11.5.2–11.5.6. Throughout the derivation, for each integer $n \geq 1$, let

$w_n =$ the number of iterations of the **while** loop in a *worst-case* execution of the binary search algorithm for an input array of length n.

The first issue to consider is this. If the length of the input array for one iteration of the **while** loop is known, what is the greatest possible length of the array input to the next iteration?

Example 11.5.2 **The Length of the Input Array to the Next Iteration of the Loop**

Prove that if an array of length k is input to the **while** loop of the binary search algorithm, then after one unsuccessful iteration of the loop, the input to the next iteration is an array of length at most $\lfloor k/2 \rfloor$.

Solution Consider what occurs when an array of length k is input to the **while** loop in the case where $x \neq a[mid]$:

$$\underbrace{a[bot],\ a[bot+1],\ \ldots,\ a[mid-1]}_{\text{new input to the while loop if } x < a[mid]},\quad \underbrace{a[mid]}_{\text{“middle element”}},\quad \underbrace{a[mid+1],\ \ldots,\ a[top-1],\ a[top]}_{\text{new input to the while loop if } x > a[mid]}.$$

Since the input array has length k, the value of *mid* depends on whether k is odd or even. In both cases we match up the array elements with the integers from 1 to k and analyze the lengths of the left and right subarrays. In case k is odd, both the left and the right subarrays have length $\lfloor k/2 \rfloor$. In case k is even, the left subarray has length $\lfloor k/2 \rfloor - 1$ and the right subarray has length $\lfloor k/2 \rfloor$. The reasoning behind these results is shown in Figure 11.5.3.

Because the maximum of the numbers $\lfloor k/2 \rfloor$ and $\lfloor k/2 \rfloor - 1$ is $\lfloor k/2 \rfloor$, in the worst case this will be the length of the array input to the next iteration of the loop. ■

To find the order of the algorithm, an explicit formula for $w_1, w_2, w_3, \ldots$ is needed. The next example derives a recurrence relation for the sequence.

Example 11.5.3 **A Recurrence Relation for $w_1, w_2, w_3, \ldots$**

Prove that the sequence $w_1, w_2, w_3, \ldots$ satisfies the recurrence relation and initial condition

$$w_1 = 1,$$
$$w_k = 1 + w_{\lfloor k/2 \rfloor} \quad \text{for every integer } k > 1.$$

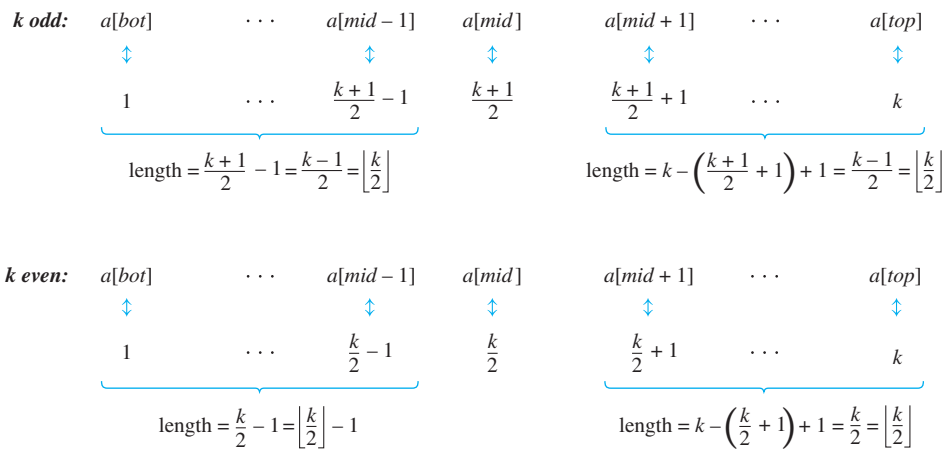


FIGURE 11.5.3 Lengths of the Left and Right Subarrays

Solution In Example 11.5.2 it was shown that given an input array of length k to the **while** loop, the worst that can happen is that the next iteration of the loop will have to search an array of length $\lfloor k/2 \rfloor$. Hence the maximum number of iterations of the loop is 1 more than the maximum number necessary to execute it for an input array of length $\lfloor k/2 \rfloor$. In symbols,

$$w_k = 1 + w_{\lfloor k/2 \rfloor}.$$

Also

$$w_1 = 1$$

because for an input array of length 1 ($bot = top$), the **while** loop iterates only one time. ■

Now that a recurrence relation for $w_1, w_2, w_3, \ldots$ has been found, iteration can be used to come up with a good guess for an explicit formula.

Example 11.5.4 **An Explicit Formula for $w_1, w_2, w_3, \ldots$**

Apply iteration to the recurrence relation found in Example 11.5.3 to conjecture an explicit formula for $w_1, w_2, w_3, \ldots$

Solution Begin by iterating to find the values of the first few terms of the sequence.

$$\begin{aligned}
w_{\textcircled{1}} &= \textcircled{1} && 1 = 2^0 \colon 1 = 0 + 1\\
w_{\textcircled{2}} &= 1 + w_{\lfloor 2/2 \rfloor} = 1 + w_1 = 1 + 1 = \textcircled{2} && 2 = 2^1 \colon 2 = 1 + 1\\
w_3 &= 1 + w_{\lfloor 3/2 \rfloor} = 1 + w_1 = 1 + 1 = 2 &&\\
w_{\textcircled{4}} &= 1 + w_{\lfloor 4/2 \rfloor} = 1 + w_2 = 1 + 2 = \textcircled{3} && 4 = 2^2 \colon 3 = 2 + 1\\
w_5 &= 1 + w_{\lfloor 5/2 \rfloor} = 1 + w_2 = 1 + 2 = 3 &&\\
w_6 &= 1 + w_{\lfloor 6/2 \rfloor} = 1 + w_3 = 1 + 2 = 3 &&\\
w_7 &= 1 + w_{\lfloor 7/2 \rfloor} = 1 + w_3 = 1 + 2 = 3 &&\\
w_{\textcircled{8}} &= 1 + w_{\lfloor 8/2 \rfloor} = 1 + w_4 = 1 + 3 = \textcircled{4} && 8 = 2^3 \colon 4 = 3 + 1\\
w_9 &= 1 + w_{\lfloor 9/2 \rfloor} = 1 + w_4 = 1 + 3 = 4 &&\\
&\vdots \qquad\qquad \vdots &&\\
w_{15} &= 1 + w_{\lfloor 15/2 \rfloor} = 1 + w_7 = 1 + 3 = 4 &&\\
w_{\textcircled{16}} &= 1 + w_{\lfloor 16/2 \rfloor} = 1 + w_8 = 1 + 4 = \textcircled{5} && 16 = 2^4 \colon 5 = 4 + 1\\
&\vdots \qquad\qquad \vdots &&
\end{aligned}$$

Note that in each case when the subscript n is between two powers of 2, w_n is 1 more than the exponent of the lower power of 2. In other words:

$$\text{If } 2^i \le n < 2^{i+1}, \text{ then } w_n = i + 1. \qquad 11.5.1$$

Now if $$2^i \le n < 2^{i+1},$$

then *[by property (11.4.2) of Example 11.4.1]*

$$i = \lfloor \log_2 n \rfloor.$$

Substituting into statement (11.5.1) gives the conjecture that

$$w_n = \lfloor \log_2 n \rfloor + 1$$ ■

Mathematical induction can then be used to verify the correctness of the formula found in Example 11.5.4.

Example 11.5.5 **Verifying the Correctness of the Formula**

Use strong mathematical induction to show that if $w_1, w_2, w_3, \ldots$ is a sequence of numbers that satisfies the recurrence relation and initial condition

$$w_1 = 1 \qquad \text{and} \qquad w_k = 1 + w_{\lfloor k/2 \rfloor} \quad \text{for each integer } k > 1,$$

then $w_1, w_2, w_3, \ldots$ satisfies the formula

$$w_n = \lfloor \log_2 n \rfloor + 1 \quad \text{for every integer } n \ge 1.$$

Solution Let $w_1, w_2, w_3, \ldots$ be the sequence defined by specifying that $w_1 = 1$ and $w_k = 1 + w_{\lfloor k/2 \rfloor}$ for each integer $k \ge 2$, and let the property $P(n)$ be the equation

$$w_n = \lfloor \log_2 n \rfloor + 1. \quad \leftarrow P(n)$$

We will use strong mathematical induction to prove that for every integer $n \ge 1$, $P(n)$ is true.

Show that P(1) is true: By definition of $w_1, w_2, w_3, \ldots$, we have that $w_1 = 1$. But $\lfloor \log_2 1 \rfloor + 1 = 0 + 1 = 1$ also. Thus $w_1 = \lfloor \log_2 1 \rfloor + 1$ and $P(1)$ is true.

Show that for every integer k > 1, if P(i) is true for each integer i from 1 through k, then P(k + 1) is also true: Let k be any integer with $k \ge 1$, and suppose that

$$w_i = \lfloor \log_2 i \rfloor + 1 \quad \text{for each integer } i \text{ with } 1 \le i \le k. \quad \leftarrow \text{inductive hypothesis}$$

We must show that

$$w_{k+1} = \lfloor \log_2 (k+1) \rfloor + 1. \quad \leftarrow P(k+1)$$

Consider the two cases: k is even and k is odd.

Case 1 (k is even): In this case, $k + 1$ is odd, and

$$\begin{aligned}
w_{k+1} &= 1 + w_{\lfloor (k+1)/2 \rfloor} && \text{by definition of } w_1, w_2, w_3, \ldots \\
&= 1 + w_{\lfloor k/2 \rfloor} && \text{because } \lfloor (k+1)/2 \rfloor = k/2 \text{ since } k+1 \text{ is odd} \\
&= 1 + (\lfloor \log_2 (k/2) \rfloor + 1) && \text{by inductive hypothesis because, since } k \text{ is even, } k \ge 2, \text{ and so } 1 \le \lfloor k/2 \rfloor \le k/2 < k \\
&= \lfloor \log_2 (k) - \log_2 2 \rfloor + 2 && \text{by substituting into the identity } \log_b (x/y) = \log_b x - \log_b y \text{ from Theorem 7.2.1} \\
&= \lfloor \log_2 (k) - 1 \rfloor + 2 && \text{since } \log_2 2 = 1
\end{aligned}$$

$$= (\lfloor \log_2 (k) \rfloor - 1) + 2 \qquad \text{by substituting } x = \log_2(k) \text{ into the identity } \lfloor x - 1 \rfloor = \lfloor x \rfloor - 1 \text{ derived in exercise 15 of Section 4.6}$$

$$= \lfloor \log_2 (k+1) \rfloor + 1 \qquad \text{by property (11.4.3) in Example 11.4.2.}$$

Case 2 (k is odd): In this case, it can also be shown that $w_k = \lfloor \log_2 k \rfloor + 1$. The analysis is very similar to that of case 1 and is left as exercise 16 at the end of the section.

Hence regardless of whether k is even or k is odd,

$$w_{k+1} = \lfloor \log_2 (k+1) \rfloor + 1,$$

as was to be shown. *[Since both the basis and the inductive steps have been demonstrated, the proof by strong mathematical induction is complete.]* ■

The final example shows how to use the formula for $w_1, w_2, w_3, \ldots$ to find a worst-case order for the algorithm.

Example 11.5.6 **The Binary Search Algorithm Is Logarithmic**

By Example 11.5.5,

$$w_n = \lfloor \log_2 n \rfloor + 1 \quad \text{for every integer } n \geq 1.$$

Use this result to show that in the worst case, the binary search algorithm is $\Theta(\log_2 n)$.

Solution Let $\Rightarrow$ stand for the words "which implies that." Then for each integer $n \geq 2$,

$$w_n = \lfloor \log_2 n \rfloor + 1 \qquad \text{by Example 11.5.5}$$

$$\Rightarrow \quad \log_2 n \leq w_n \leq \log_2 n + 1 \qquad \text{because } x < \lfloor x \rfloor + 1 \text{ and } \lfloor x \rfloor \leq x \text{ for every real number } x$$

$$\Rightarrow \quad \log_2 n \leq w_n \leq \log_2 n + \log_2 n \qquad \text{since the logarithm with base 2 is increasing, when } 2 \leq n, \text{ then } 1 = \log_2 2 \leq \log_2 n.$$

$$\Rightarrow \quad \log_2 n \leq w_n \leq 2\log_2 n.$$

Let $A = 1$, $B = 2$, and $k = 2$. Then

$$A \log_2 n \leq w_n \leq B \log_2 n \quad \text{for every integer } n \geq k.$$

Hence by definition of Θ-notation,

$$w_n \quad \text{is} \quad \Theta(\log_2 n).$$

Finally, because w_n, the number of iterations of the **while** loop, is proportional to the number of comparisons performed when the binary search algorithm is executed, the binary search algorithm is $\Theta(\log_2 n)$. ■

Examples 11.5.2–11.5.6 show that in the worst case, the binary search algorithm has order $\log_2 n$. As noted in Section 11.3, in the worst case the sequential search algorithm has order n. This difference in efficiency becomes increasingly more important as n gets larger and larger. If one loop iteration is performed each nanosecond, then performing n iterations for $n = 100{,}000{,}000$ requires 0.1 second, whereas performing $\log_2 n$ iterations requires 0.000000027 second. For $n = 100{,}000{,}000{,}000$ the times are 1.67 minutes and 0.000000037 second, respectively. And for $n = 100{,}000{,}000{,}000{,}000$ the respective times are 27.78 hours and 0.000000047 second.

Merge Sort

Note that it is much easier to write a detailed algorithm for sequential search than for binary search. Yet binary search is much more efficient than sequential search. Such trade-offs

often occur in computer science. Frequently, the straightforward "obvious" solution to a problem is less efficient than a clever solution that is more complicated to describe.

In the text and exercises for Section 11.3, we gave two methods for sorting, insertion sort and selection sort, both of which are formalizations of methods human beings often use in ordinary situations. Can a divide-and-conquer approach be used to find a sorting method more efficient than these? It turns out that the answer is an emphatic "yes." In fact, over the past few decades, computer scientists have developed several divide-and-conquer sorting methods all of which are somewhat more complex to describe but are significantly more efficient than either insertion sort or selection sort.

One of these methods, **merge sort**, is obtained by thinking recursively. Imagine that an efficient way for sorting arrays of length less than k is already known. How can such knowledge be used to sort an array of length k? One way is to suppose the array of length k is split into two roughly equal parts and each part is sorted using the known method. Is there an efficient way to combine the parts into a sorted array? Sure. Just "merge" them.

Figure 11.5.4 illustrates how a merge works. Imagine that the elements of two ordered subarrays—2, 5, 6, 8 and 3, 6, 7, 9—are written on slips of paper (to make them easy to move around). Place the slips for each subarray in two columns on a tabletop, one at the left and one at the right. Along the bottom of the tabletop, set up eight positions into which the slips will be moved. Then, one-by-one, bring down the slips from the bottoms of the columns. At each stage compare the numbers on the slips currently at the column bottoms, and move the slip containing the smaller number down into the next position in the array as a whole. If at any stage the two numbers are equal, take, say, the slip on the left to move into the next position. And if one of the columns is empty at any stage, just move all the slips from the other column into the correct positions one-by-one in order.

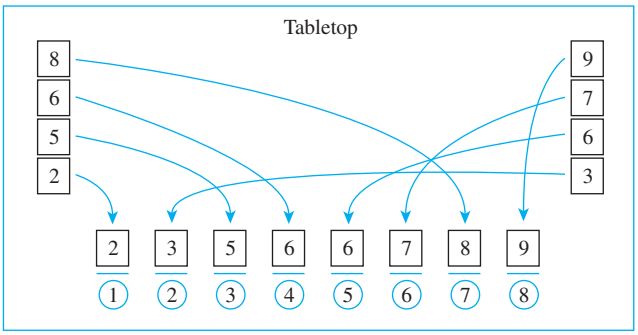


FIGURE 11.5.4 Merging Two Sorted Subarrays to Obtain a Sorted Array

The process of merging is efficient because the total number of comparisons needed to merge two subarrays into an array of length k is just $k - 1$. You can see why by analyzing Figure 11.5.4. Observe that at each stage, the decision about which slip to move is made by comparing the numbers on the slips currently at the bottoms of the two columns—except when one of the columns is empty, in which case no comparisons are made at all. Thus in the worst case there will be one comparison for each of the k positions in the final array except the very last one (because when the last slip is placed into position, the other column is sure to be empty), or a total of $k - 1$ comparisons in all.

The merge sort algorithm is recursive because its defining statements include references to itself. The algorithm is well defined, however, because at each stage the length of the array that is input to the algorithm is shorter than at the previous stage, so that, ultimately, the algorithm has to deal only with arrays of length 1, which are already sorted. Specifically, merge sort works as follows.

Given an array of elements that can be put into order, if the array consists of a single element, leave it as it is. It is already sorted. Otherwise:

1. Divide the array into two subarrays of as nearly equal length as possible.
2. Use merge sort to sort each subarray.
3. Merge the two subarrays together.

Figure 11.5.5 illustrates a merge sort in a particular case.

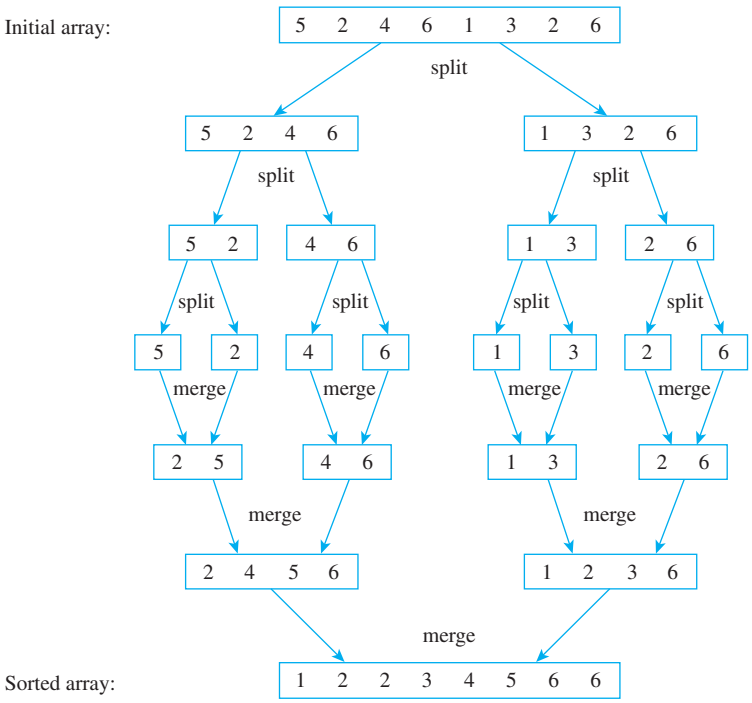


FIGURE 11.5.5 Applying Merge Sort to the Array 5, 2, 4, 6, 1, 3, 2, 6

As in the case of the binary search algorithm, in order to formalize merge sort we must decide at exactly what point to split each array. Given an array denoted by $a[bot], a[bot+1], \ldots, a[top]$, let $mid = \lfloor (bot + top)/2 \rfloor$. Take the left subarray to be $a[bot], a[bot+1], \ldots, a[mid]$ and the right subarray to be $a[mid+1], a[mid+2], \ldots, a[top]$. The following is a formal version of merge sort.

Algorithm 11.5.2 Merge Sort

[The aim of this algorithm is to take an array of elements $a[r], a[r+1], \ldots, a[s]$ (where $r \le s$) and to order it. The output array is denoted $a[r], a[r+1], \ldots, a[s]$ also. It has the same values as the input array, but they are in ascending order. The input array is split into two nearly equal-length subarrays, each of which is ordered using merge sort. Then the two subarrays are merged together.]

Input: r and s *[positive integers with $r \le s$], $a[r], a[r+1], \ldots, a[s]$ [an array of data items that can be ordered]*

Algorithm Body:

bot := *r*, *top* := *s*
while (*bot* < *top*)

$$mid := \left\lfloor \frac{bot + top}{2} \right\rfloor$$

call **merge sort** with input *bot*, *mid*, and
a[*bot*], *a*[*bot* + 1], . . . , *a*[*mid*]
call **merge sort** with input *mid* + 1, *top* and
a[*mid* + 1], *a*[*mid* + 2], . . . , *a*[*top*]

[After these steps are completed, both arrays a[bot], a[bot + 1], . . . , a[mid] and a[mid + 1], a[mid + 2], . . . , a[top] are in order.]

merge *a*[*bot*], *a*[*bot* + 1], . . . , *a*[*mid*] and *a*[*mid* + 1], *a*[*mid* + 2], . . . , *a*[*top*]

[This step can be done with a call to a merge algorithm. To put the final array in ascending order, the merge algorithm must be written so as to take two arrays in ascending order and merge them into an array in ascending order.]

end while

Output: *a*[*r*], *a*[*r* + 1], . . . , *a*[*s*] *[an array with the same elements as the input array but in ascending order]*

To derive the efficiency of merge sort, let

m_n = the maximum number of comparisons used when merge sort is applied to an array of length n.

Then $m_1 = 0$ because no comparisons are used when merge sort is applied to an array of length 1. Also for any integer $k > 1$, consider an array $a[bot], a[bot + 1], \ldots, a[top]$ of length k that is split into two subarrays, $a[bot], a[bot + 1], \ldots, a[mid]$ and $a[mid + 1], a[mid + 2], \ldots, a[top]$, where $mid = \lfloor (bot + top)/2 \rfloor$. In exercise 24 you are asked to show that the right subarray has length $\lfloor k/2 \rfloor$ and the left subarray has length $\lceil k/2 \rceil$. From the previous discussion of the merge process, it is known that to merge two subarrays into an array of length k, at most $k - 1$ comparisons are needed.

Consequently,

$$\begin{bmatrix}\text{the number of comparisons}\\ \text{when merge sort is applied}\\ \text{to an array of length } k\end{bmatrix} = \begin{bmatrix}\text{the number of comparisons}\\ \text{when merge sort is applied}\\ \text{to an array of length } \lfloor k/2 \rfloor\end{bmatrix} + \begin{bmatrix}\text{the number of comparisons}\\ \text{when merge sort is applied}\\ \text{to an array of length } \lceil k/2 \rceil\end{bmatrix} + \begin{bmatrix}\text{the number of comparisons}\\ \text{used to merge two subarrays}\\ \text{into an array of length } k.\end{bmatrix}$$

In other words,

$$m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + (k - 1) \quad \text{for every integer } k > 1.$$

In exercise 25 you are asked to use this recurrence relation to show that

$$\frac{1}{2} n \log_2 n \leq m_n \leq 2n \log_2 n \quad \text{for every integer } n \geq 1.$$

It follows that merge sort is $\Theta(n \log_2 n)$.

In the text and exercises for Section 11.3, we showed that insertion sort and selection sort are both $\Theta(n^2)$. How much difference can it make that merge sort is $\Theta(n \log_2 n)$? If $n = 100{,}000{,}000$ and a computer is used that performs one operation each nanosecond, the time needed to perform $n \log_2 n$ operations is about 2.7 seconds, whereas the time needed to perform n^2 operations is over 115 days.

Tractable and Intractable Problems

At an opposite extreme from an algorithm such as binary search, which has logarithmic order, is an algorithm with exponential order. For example, consider an algorithm to direct the movement of each of the 64 disks in the Tower of Hanoi puzzle as they are transferred one by one from one pole to another. In Section 5.7 we showed that such a transfer requires $2^{64} - 1$ steps. If a computer took a nanosecond to calculate each transfer step, the total time to calculate all the steps would be

$$(2^{64} - 1) \cdot \left(\frac{1}{10^9}\right) \cdot \left(\frac{1}{60}\right) \cdot \left(\frac{1}{60}\right) \cdot \left(\frac{1}{24}\right) \cdot \left(\frac{1}{365.25}\right) \cong 584.5 \text{ years.}$$

number of moves; moves per second; seconds per minute; minutes per hour; hours per day; days per year

Problems whose solutions can be found with algorithms whose worst-case order with respect to time is a polynomial are said to belong to **class P**. They are called **polynomial-time algorithms** and are said to be **tractable**. Problems that cannot be solved in polynomial time are called **intractable**. For certain problems, it is possible to check the correctness of a proposed solution with a polynomial-time algorithm, but it may not be possible to find a solution in polynomial time. Such problems are said to belong to **class NP**.* The biggest open question in theoretical computer science is whether every problem in class NP belongs to class P. This is known as the **P vs. NP** problem. The Clay Institute, in Cambridge, Massachusetts, has offered a prize of $1,000,000 to anyone who can either prove or disprove that P = NP.

In recent years, computer scientists have identified a fairly large set of problems, called **NP-complete**, that all belong to class NP but are widely believed not to belong to class P. What is known for sure is that if any one of these problems is solvable in polynomial time, then so are all the others. One of the NP-complete problems, commonly known as the *traveling salesman problem*, was discussed in Section 10.1.

A Final Remark on Algorithm Efficiency

This section and the previous one on algorithm efficiency have offered only a partial view of what is involved in analyzing a computer algorithm. For one thing, it is assumed that searches and sorts take place in the memory of the computer. Searches and sorts on

*Technically speaking, a problem whose solution can be verified on an ordinary computer (or *deterministic sequential machine*) with a polynomial-time algorithm can be solved on a *nondeterministic sequential machine* with a polynomial-time algorithm. Such problems are called NP, which stands for *nondeterministic polynomial-time algorithm*.

disk-based files require different algorithms, though the methods for their analysis are similar. For another thing, as mentioned at the beginning of Section 11.3, time efficiency is not the only factor that matters in the decision about which algorithm to choose. Although computer memory is now very inexpensive, the amount of memory space required may also be a factor. There are mathematical techniques to estimate space efficiency, which are very similar to those used to estimate time efficiency. Furthermore, as parallel processing of data becomes increasingly prevalent, current methods of algorithm analysis are being modified and extended to apply to algorithms designed for this new technology.

TEST YOURSELF

1. To solve a problem using a divide-and-conquer algorithm, you reduce it to a fixed number of smaller problems of the same kind, which can themselves be _____, and so forth until _____.
2. To search an array using the binary search algorithm in each step, you compare a middle element of the array to _____. If the middle element is less than _____, you _____, and if the middle element is greater than _____, you _____.
3. The worst-case order of the binary search algorithm is _____.
4. To sort an array using the merge sort algorithm, in each step until the last one you split the array into approximately two equal sections and sort each section using _____. Then you _____ the two sorted sections.
5. The worst-case order of the merge sort algorithm is _____.

EXERCISE SET 11.5

1. Use the facts that $\log_2 10 \cong 3.32$ and that for each real number a, $\log_2(10^a) = a \log_2 10$ to find $\log_2(1{,}000)$, $\log_2(1{,}000{,}000)$, and $\log_2(1{,}000{,}000{,}000{,}000)$.
2. Suppose an algorithm requires $c\lfloor \log_2 n \rfloor$ operations when performed with an input of size n (where c is a constant).
   a. By what factor will the number of operations increase when the input size is increased from m to m^2 (where m is a positive integer power of 2)?
   b. By what factor will the number of operations increase when the input size is increased from m to m^{10} (where m is a positive integer power of 2)?
   c. When n increases from 128 $(= 2^7)$ to 268,435,456 $(= 2^{28})$, by what factor is $c\lfloor \log_2 n \rfloor$ increased?

Exercises 3 and 4 illustrate that for relatively small values of *n*, algorithms with larger orders can be more efficient than algorithms with smaller orders. Use a graphing calculator or computer to answer these questions.

3. For what values of n is an algorithm that requires n operations more efficient than an algorithm that requires $\lfloor 50 \log_2 n \rfloor$ operations?
4. For what values of n is an algorithm that requires $\lfloor n^2/10 \rfloor$ operations more efficient than an algorithm that requires $\lfloor n \log_2 n \rfloor$ operations?

In 5 and 6, trace the action of the binary search algorithm (Algorithm 11.5.1) on the variables *index*, *bot*, *top*, *mid*, and the given values of *x* for the input array *a*[1] = Chia, *a*[2] = Doug, *a*[3] = Jan, *a*[4] = Jim, *a*[5] = Jose, *a*[6] = Mary, *a*[7] = Rob, *a*[8] = Roy, *a*[9] = Sue, *a*[10] = Usha, where alphabetical ordering is used to compare elements of the array.

5. **a.** x = Chia **b.** x = Max
6. **a.** x = Amanda **b.** x = Roy
7. Suppose *bot* and *top* are positive integers with $bot \le top$. Consider the array

$$a[bot],\ a[bot+1],\ \ldots,\ a[top].$$

   a. How many elements are in this array?
   b. Show that if the number of elements in the array is odd, then the quantity $bot + top$ is even.

c. Show that if the number of elements in the array is even, then the quantity $bot + top$ is odd.

Exercises 8–11 refer to the following algorithm segment. For each positive integer n, let a_n be the number of iterations of the while loop.

while $(n > 0)$
$n := n \text{ div } 2$
end while

8. Trace the action of this algorithm segment on n when the initial value of n is 27.

9. Find a recurrence relation for a_n.

10. Find an explicit formula for a_n.

11. Find an order for this algorithm segment.

Exercises 12–15 refer to the following algorithm segment. For each positive integer n, let b_n be the number of iterations of the while loop.

while $(n > 0)$
$n := n \text{ div } 3$
end while

12. Trace the action of this algorithm segment on n when the initial value of n is 424.

13. Find a recurrence relation for b_n.

***H* 14.** **a.** Use iteration to guess an explicit formula for b_n.

b. Prove that if k is an integer and x is a real number with $3^k \le x < 3^k$, then $\lfloor \log_3 x \rfloor = k$.

c. Prove that for every integer $m \ge 1$,

$$\lfloor \log_3(3m) \rfloor = \lfloor \log_3(3m+1) \rfloor = \lfloor \log_3(3m+2) \rfloor.$$

d. Prove the correctness of the formula you found in part (a).

15. Find an order for the algorithm segment.

16. Complete the proof of case 2 of the strong induction argument in Example 11.5.5. In other words, show that if k is an odd integer and $w_i = \lfloor \log_2 i \rfloor + 1$ for every integer i with $1 \le i \le k$, then $w_{k+1} = \lfloor \log_2 k + 1 \rfloor + 1$.

For 17–19, modify the binary search algorithm (Algorithm 11.5.1) to take the upper of the two middle array elements in case the input array has even length. In other words, in Algorithm 11.5.1 replace

$$mid := \left\lfloor \frac{bot + top}{2} \right\rfloor \text{ with } mid := \left\lceil \frac{bot + top}{2} \right\rceil.$$

17. Trace the modified binary search algorithm for the same input as was used in Example 11.5.1.

18. Suppose an array of length k is input to the **while** loop of the modified binary search algorithm. Show that after one iteration of the loop, if $a[mid] \ne x$, the input to the next iteration is an array of length at most $\lfloor k/2 \rfloor$.

19. Let w_n be the number of iterations of the **while** loop in a worst-case execution of the modified binary search algorithm for an input array of length n. Show that $w_k = 1 + w_{\lfloor k/2 \rfloor}$ for $k \ge 2$.

In 20 and 21, draw a diagram like Figure 11.5.4 to show how to merge the given subarrays into a single array in ascending order.

20. 3, 5, 6, 9, 12 and 2, 4, 7, 9, 11

21. F, K, L, R, U and C, E, L, P, W (alphabetical order)

In 22 and 23, draw a diagram like Figure 11.5.5 to show how merge sort works for the given input arrays.

22. R, G, B, U, C, F, H, G (alphabetical order)

23. 5, 2, 3, 9, 7, 4, 3, 2

24. Show that given an array $a[bot], a[bot+1], \ldots, a[top]$ of length k, if mid $= \lfloor (bot + top)/2 \rfloor$ then

a. the subarray $a[mid+1], a[mid+2], \ldots, a[top]$ has length $\lfloor k/2 \rfloor$.

b. the subarray $a[bot], a[bot+1], \ldots, a[mid]$ has length $\lceil k/2 \rceil$.

***H* 25.** The recurrence relation for $m_1, m_2, m_3, \ldots$, which arises in the calculation of the efficiency of merge sort, is

$$m_1 = 0$$
$$m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1.$$

Show that for every integer $n \ge 1$,

a. $\frac{1}{2} n \log_2 n \le m_n$

b. $m_n \le 2n \log_2 n$

26. It might seem that $n - 1$ multiplications are needed to compute x^n, since

$$x_n = \underbrace{x \cdot x \cdot \cdots x}_{n-1 \text{ multiplications}}.$$

But observe that, for instance, since $6 = 4 + 2$,

$$x^6 = x^4 x^2 = (x^2)^2 x^2.$$

Thus x^6 can be computed using three multiplications: one to compute x^2, one to compute $(x^2)^2$,

and one to multiply $(x^2)^2$ times x^2. Similarly, since $11 = 8 + 2 + 1$,

$$x^{11} = x^8x^2x^1 = ((x^2)^2)^2x^2x$$

and so x^{11} can be computed using five multiplications: one to compute x^2, one to compute $(x^2)^2$, one to compute $((x^2)^2)^2$, one to multiply $((x^2)^2)^2$ times x^2, and one to multiply that product by x.

a. Write an algorithm to take a real number x and a positive integer n and compute x^n by
   (i) calling Algorithm 5.1.1 to find the binary representation of n:

$$(r[k]\ r[k-1]\cdots r[0])_2,$$

   where each $r[i]$ is 0 or 1;
   (ii) computing $x^2, x^{2^2}, x^{2^3}, \ldots, x^{2^k}$ by squaring, then squaring again, and so forth;
   (iii) computing x^n using the fact that

$$x^n = x^{r[k]2^k + \cdots + r[2]2^2 + r[1]2^1 + r[0]2^0}$$

$$= x^{r[k]2^k} \cdots x^{r[2]2^2} \cdot x^{r[1]2^1} \cdot x^{r[0]2^0}$$

b. Show that the number of multiplications performed by the algorithm of part (a) is less than or equal to $2\lfloor \log_2 n \rfloor$.

ANSWERS FOR TEST YOURSELF

1. reduced to the same finite number of smaller problems of the same kind; easily resolved problems are obtained **2.** the element you are looking for; the element you are looking for; apply the binary search algorithm to the lower half of the array; the element you are looking for; apply the binary search algorithm to the upper half of the array **3.** $\log_2 n$, where n is the length of the array **4.** merge sort; merge **5.** $n \log_2 n$

CHAPTER 12

REGULAR EXPRESSIONS AND FINITE-STATE AUTOMATA

The theoretical foundations of computer science are derived from several disciplines: logic (the foundations of mathematics), electrical engineering (the design of switching circuits), brain research (models of neurons), and linguistics (the formal specification of languages).

As discussed briefly in Sections 6.4 and 7.4, the 1930s saw the development of mathematical treatments of basic questions concerning what can be proved in mathematics and what can be computed by means of a finite sequence of mechanized operations. Although the first digital computers were not built until the early 1940s, ten years earlier Alan Turing developed a simple abstract model of a machine, now called a Turing machine, by means of which he defined what it would mean for a function to be computable.

Around the same time, somewhat similar models of computation were developed by the American logicians Alonzo Church, Stephen C. Kleene, and Emil Post (who was born in Poland but came to the United States as a child), but Church and others showed these all to be equivalent. As a result, Church formulated a conjecture, now known as the **Church-Turing thesis**, asserting that the Turing machine is universal in the sense that anything that can ever be computed on a machine can be computed with a Turing machine. If this thesis is correct—which is widely believed—then all computers that have been or will ever be constructed are theoretically equivalent in what they can do, although they may differ widely in speed and storage capacity. For instance, quantum computers may have the capability to compute certain quantities enormously faster than classical computers. But Church's thesis implies that the theory of computation is likely to remain fundamentally the same, even though the enabling technology is subject to constant change.

In the early 1940s, Warren S. McCulloch and Walter Pitts, working at the Massachusetts Institute of Technology (M.I.T.), developed a model of how the neurons in the brain might work and how models of neurons could be combined to make "circuits" or "automata" capable of more complicated computations. To a certain extent, they were influenced by the results of Claude Shannon, who also worked at M.I.T. and had in the 1930s developed the foundations of a theory that implemented Boolean functions as switching circuits. In the 1950s, Kleene analyzed the work of McCulloch and Pitts and connected it with versions of the machine models introduced by Turing and others.

Another development of the 1950s was the introduction of high-level computer languages. During the same years, linguist Noam Chomsky's attempts to understand the underlying principles by means of which human beings generate speech led him to develop a theory of formal languages, which he defined using sets of abstract rules, called *grammars*, of varying levels of complexity. It soon became apparent that Chomsky's theory was of great utility in the analysis and construction of computer languages. For computer science, the most useful of Chomsky's language classifications are also the two simplest: the *regular languages* and the *context-free languages.*

Regular languages, which are defined by *regular expressions*, are used extensively for matching patterns within text (as in word processing or Internet searches) and for lexical analysis in computer language compilers. They are part of sophisticated text editors and a number of UNIX* utilities, and they are also used in transforming XML† documents.

Using the Backus-Naur notation (introduced in Section 10.4), context-free languages can describe many of the more complex aspects of modern high-level computer languages, and they form the basis for a key part of compilers, which translate programs written in a high-level language into machine code suitable for execution.

A remarkable fact is that all of the subjects referred to previously are related. Each context-free grammar turns out to be equivalent to a type of automaton called a *pushdown automaton*, and each regular expression turns out to be equivalent to a type of automaton called a *finite-state automaton*. In this chapter, we focus on the study of regular languages and finite-state automata, leaving the subject of context-free grammars and their equivalent automata to a later course in compiler construction or automata theory.

Note Automaton is pronounced aw-TAHM-uh-than. The plural of automaton is automata.

12.1 Formal Languages and Regular Expressions

The mind has finite means but it makes unbounded use of them and in very specific and organized ways. That's the core problem of language that it became possible to face [*by the mid-twentieth century*]. —Noam Chomsky, circa 1998

DPA Picture Alliance Archive/Alamy Stock Photo

Noam Chomsky (born 1928)

An English sentence can be regarded as a string of words, and an English word can be regarded as a string of letters. Not every string of letters is a legitimate word, and not every string of words is a grammatical sentence. We could say that a word is legitimate if it can be found in an unabridged English dictionary and that a sentence is grammatical if it satisfies the rules in a standard English grammar book.

Computer languages are similar to English in that certain strings of characters are legitimate words of the language and certain strings of words can be put together according to certain rules to form syntactically correct programs. A compiler for a computer language analyzes the stream of characters in a program—first to recognize individual word and sentence units (this part of the compiler is called a lexical scanner), then to analyze the syntax, or grammar, of the sentences (this part is called a syntactic analyzer), and finally to translate the sentences into machine code (this part is called a code generator).

In computer science it has proved useful to look at languages from a very abstract point of view as strings of certain fundamental units and allow any finite set of symbols to be used as an alphabet. It is common to denote an alphabet by a capital Greek sigma: Σ. (This just happens to be the same symbol as the one used for summation, but the two concepts have no other connection.)

In Section 5.9 we used recursion to give a formal definition for strings over an alphabet, and we used structural induction to give rigorous proofs for their properties. The formal definition provides a solid foundation for picturing strings as juxtapositions of characters.

*UNIX is an operating system that was developed in 1969 by Kenneth Thompson at Bell Laboratories. Originally written in assembly language, it was later rewritten in Dennis Ritchie's C language, which was also developed at Bell Laboratories.

†XML is a standard for defining markup languages used for Internet applications.

Note A Greek sigma is the traditional symbol used to denote an alphabet in a formal language. It is smaller than the Greek sigma used for a summation.

Alphabet Σ:	a finite set of characters
String over Σ:	(1) a finite juxtaposition of elements (called **characters**) of Σ or (2) the null string λ
Length of a string over Σ:	the number of characters that made up the string, with the null string having length 0
Formal language over Σ:	a set of strings over the alphabet

Note that the empty set satisfies the criteria for being a formal language. Allowing the empty set to be a formal language turns out to be convenient in certain technical situations.

Example 12.1.1 **Examples of Formal Languages**

Let the alphabet $\Sigma = \{a, b\}$.

a. Define a language L_1 over Σ to be the set of all strings that begin with the character a and have length at most three characters. Find L_1.

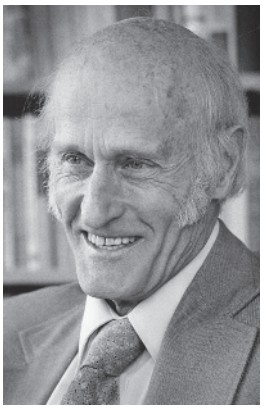
b. A **palindrome** is a string that looks the same if the order of its characters is reversed. For instance, *aba* and *baab* are palindromes. Define a language L_2 over Σ to be the set of all palindromes obtained using the characters of Σ. Write ten elements of L_2.

Solution

a. $L_1 = \{a, aa, ab, aaa, aab, aba, abb\}$

b. L_2 contains the following ten strings (among infinitely many others):

$$\lambda, a, b, aa, bb, aaa, bab, abba, babaabab, abaabbbbbaaba$$ ■



Stephen C. Kleene (1909–1994)

University of Wisconsin Digital Collections Center

Notation

Let Σ be an alphabet. For each nonnegative integer n, let

Σ^n = the set of all strings over Σ that have length n,
Σ^+ = the set of all strings over Σ that have length at least 1, and
Σ^* = the set of all strings over Σ.

Note that Σ^n is essentially the Cartesian product of n copies of Σ. The language Σ^* is called the **Kleene closure of Σ**, in honor of Stephen C. Kleene (pronounced CLAY-nee). Σ^+ is the set of all strings over Σ except for λ and is called the **positive closure of Σ**.

Example 12.1.2 **The Languages Σ^n, Σ^+, and Σ^***

Let $\Sigma = \{a, b\}$.

a. Find Σ^0, Σ^1, Σ^2, and Σ^3.

b. Let $A = \Sigma^0 \cup \Sigma^1$ and $B = \Sigma^2 \cup \Sigma^3$. Use words to describe A, B, and $A \cup B$.

c. Describe a systematic way of writing the elements of Σ^+. What change needs to be made to obtain the elements of Σ^*?

Solution

a. $\Sigma^0 = \{\lambda\}$, $\Sigma^1 = \{a, b\}$, $\Sigma^2 = \{aa, ab, ba, bb\}$, and $\Sigma^3 = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$

b. A is the set of all strings over Σ of length at most 1.
B is the set of all strings over Σ of length 2 or 3.
$A \cup B$ is the set of all strings over Σ of length at most 3.

c. Elements of Σ^+ can be written systematically by writing all the strings of length 1, then all the strings of length 2, and so forth.

$$\Sigma^+: a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa, \ldots.$$

Of course, the process of writing the strings in Σ^+ would continue forever, because Σ^+ is an infinite set. The only change that needs to be made to obtain Σ^* is to place the null string at the beginning of the list. ■

Example 12.1.3 **Polish Notation: A Language Consisting of Postfix Expressions**

An expression such as $a + b$, in which a binary operator such as $+$ sits between the two quantities on which it acts, is said to be written in **infix notation**. Alternative notations are called **prefix notation** (in which the binary operator precedes the quantities on which it acts) and **postfix notation** (in which the binary operator follows the quantities on which it acts). In prefix notation, $a + b$ is written $+ ab$. In postfix notation, $a + b$ is written $ab +$.

Prefix and postfix notations were introduced in 1920 by the Polish mathematician Jan Łukasiewicz (pronounced Wu-ca-SHAY-vich). In his honor—and because some people have difficulty pronouncing his name—they are often referred to as **Polish notation** and **reverse Polish notation**, respectively. A great advantage of these notations is that they eliminate the need for parentheses in writing arithmetic expressions. For instance, in postfix (or reverse Polish) notation, the expression $8\ 4 + 6\ /$ is evaluated from left to right as follows: Add 8 and 4 to obtain 12, and then divide 12 by 6 to obtain 2. As another example, if the expression $(a + b) \cdot c$ in infix notation is converted to postfix notation, the result is $ab + c \cdot$.

a. If the expression $ab \cdot cd \cdot +$ in postfix notation is converted to infix notation, what is the result?

b. Let $\Sigma = \{4, 1, +, -\}$, and let $L =$ the set of all strings over Σ obtained by writing either a 4 or a 1 first, then either a 4 or a 1, and finally either a $+$ or a $-$. List all elements of L between braces, and evaluate the resulting expressions.

Solution

a. $a \cdot b + c \cdot d$

b. $L = \{4\ 1\ +, 4\ 1\ -, 1\ 4\ +, 1\ 4\ -, 4\ 4\ +, 4\ 4\ -, 1\ 1\ +, 1\ 1\ -\}$

$4\ 1+ = 4 + 1 = 5, \quad 4\ 1- = 4 - 1 = 3, \quad 1\ 4+ = 1 + 4 = 5,$

$1\ 4- = 1 - 4 = -3, \quad 4\ 4+ = 4 + 4 = 8, \quad 4\ 4- = 4 - 4 = 0,$

$1\ 1+ = 1 + 1 = 2, \quad 1\ 1- = 1 - 1 = 0$ ■

The following definition describes ways in which languages can be combined to form new languages.

Definition

Let Σ be an alphabet. Given any strings x and y over Σ, the **concatenation of x and y** is the string obtained by writing all the characters of x followed by all the characters of y. For any languages L and L' over Σ, three new languages can be defined as follows:

The **concatenation of L and L'**, denoted LL', is

$$LL' = \{xy \mid x \in L \text{ and } y \in L'\}.$$

The **union of L and L'**, denoted $L \cup L'$, is

$$L \cup L' = \{x \mid x \in L \text{ or } x \in L'\}.$$

The **Kleene closure of L**, denoted L^*, is

$$L^* = \{x \mid x \text{ is a concatenation of any finite number of strings in } L\}.$$

Note that λ is in L^* because it is regarded as a concatenation of zero strings in L.

Example 12.1.4 **New Languages from Old**

Let L_1 be the set of all strings consisting of an even number of a's (namely, λ, aa, $aaaa$, $aaaaaa, \ldots$), and let $L_2 = \{b, bb, bbb\}$. Find L_1L_2, $L_1 \cup L_2$, and $(L_1 \cup L_2)^*$. Note that the null string λ is in L_1 because 0 is an even number.

Solution

$L_1 L_2$ = the set of all strings that consist of an even number of a's followed by b or by bb or by bbb.

$L_1 \cup L_2$ = the set that includes the strings b, bb, bbb and any strings consisting of an even number of a's.

$(L_1 \cup L_2)^*$ = the set of all strings of a's and b's in which every occurrence of a is in a block consisting of an even number of a's. ■

The Language Defined by a Regular Expression

One of the most useful ways to define a language is by means of a *regular expression*, a concept first introduced by Kleene. We give a recursive definition for generating the set of all regular expressions over an alphabet.

Definition

Given an alphabet Σ, the following are **regular expressions over Σ**:

I. Base: $\varnothing$, λ, and each individual symbol in Σ are regular expressions over Σ.

II. Recursion: If r and s are regular expressions over Σ, then the following are also regular expressions over Σ:

(i) (rs) (ii) $(r \mid s)$ (iii) (r^*),

where rs denotes the concatenation of r and s, r^* denotes the concatenation of r with itself any finite number (including zero) of times, and $r \mid s$ denotes either one of the strings r or s. The regular expression r^* is called the **Kleene closure** of r.

III. Restriction: Nothing is a regular expression over Σ except for objects defined in (I) and (II) above.

As an example, one regular expression over $\Sigma = \{a, b, c\}$ is

$$a \mid (b \mid c)^* \mid (ab)^*.$$

If the alphabet Σ happens to include symbols—such as (, or |, or), or *—special provisions have to be made to avoid ambiguity. An *escape character*, usually a backslash, is added before the potentially ambiguous symbol. For instance, a left parenthesis would be written as \(and the backslash itself would be written as \\.

To eliminate parentheses, an **order of precedence** for the operations used to define regular expressions has been introduced. The highest is *, concatenation is next, and | is the lowest. It is also customary to eliminate the outer set of parentheses in a regular expression when the order of precedence rules are sufficient for avoiding ambiguity. Thus

$$(a((bc)^*)) = a(bc)^* \quad \text{and} \quad (a \mid (bc)) = a \mid bc.$$

Example 12.1.5 **Order of Precedence for the Operations in a Regular Expression**

a. Add parentheses to emphasize the order of precedence in the following expression: $ab^* \mid b^*a$.

b. Use the rules about order of precedence to eliminate the parentheses in the following expression: $((a \mid ((b^*)c))(a^*))$.

Solution

a. $((a(b^*)) \mid ((b^*)a))$ b. $(a \mid b^*c)a^*$ ■

Given a finite alphabet, every regular expression over the alphabet defines a formal language. The function from regular expressions to formal languages is defined recursively.

Definition

For any finite alphabet Σ, the function L that associates a language to each regular expression over Σ is defined by (I)–(III) below. For each such regular expression r, $L(r)$ is called the **language defined by *r***.

I. Base: $L(\varnothing) = \varnothing$, $L(\lambda) = \{\lambda\}$, $L(a) = \{a\}$ for every a in Σ.

II. Recursion: If $L(r)$ and $L(r')$ are the languages defined by the regular expressions r and r' over Σ, then

(i) $L(rr') = L(r)L(r')$ (ii) $L(r \mid r') = L(r) \cup L(r')$ (iii) $L(r^*) = (L(r))^*$.

III. Restriction: The function L is completely determined by I and II above.

Note that any finite language can be defined by a regular expression. For instance, the language {cat, dog, bird} is defined by the regular expression (cat | dog | bird). An important example is the following.

Example 12.1.6 **Using Set Notation to Describe the Language Defined by a Regular Expression**

Let $\Sigma = \{a, b\}$, and consider the language defined by the regular expression $(a \mid b)^*$. Use set notation to find this language, and describe it in words.

Solution The language defined by $(a \mid b)^*$ is

$$\begin{aligned} L((a \mid b)^*) &= (L(a \mid b))^* \\ &= (L(a) \cup L(b))^* \\ &= (\{a\} \cup \{b\})^* \\ &= \{a, b\}^* && \text{by definition of operations on languages} \\ &= \text{the set of all strings of } a\text{'s and } b\text{'s} \\ &= \Sigma^*. \end{aligned}$$

■

In Section 5.9 we proved that concatenation of strings is associative. Taking unions of sets is also an associative operation. Thus for any regular expressions r, s, and t,

$$L((rs)t) = L(r(st)),$$

and

$$\begin{aligned} L((r \mid s) \mid t) &= (L(r \mid s)) \cup L(t) && \text{by definition of } \mid \\ &= (L(r) \cup L(s)) \cup L(t) && \text{by definition of } \mid \\ &= L(r) \cup (L(s) \cup L(t)) && \text{by the associativity of union for sets} \\ &= L(r) \cup (L(s \mid t)) && \text{by definition of } \mid \\ &= L(r \mid (s \mid t)) && \text{by definition of } \mid. \end{aligned}$$

Because of these relationships, it is customary to drop the parentheses in "associative" situations and write

$$rst = (rs)t = r(st)$$

and

$$r \mid s \mid t = (r \mid s) \mid t = r \mid (s \mid t).$$

As you become accustomed to working with regular expressions, you will find that you do not need to go through a formal derivation in order to determine the language defined by an expression.

Example 12.1.7 **The Language Defined by a Regular Expression**

Let $\Sigma = \{0, 1\}$. Use words to describe the languages defined by the following regular expressions over Σ.

a. $0^*1^* \mid 1^*0^*$ b. $0(0 \mid 1)^*$

Solution

a. The strings in this language consist either of a string of 0's followed by a string of 1's or of a string of 1's followed by a string of 0's. However, in either case the strings could be empty, which means that λ is also in the language.

b. The strings in this language have to start with a 0. The 0 may be followed by any finite number (including zero) of 0's and 1's in any order. Thus the language is the set of all strings of 0's and 1's that start with a 0. ■

Example 12.1.8 **Individual Strings in the Language Defined by a Regular Expression**

In each of (a) and (b), let $\Sigma = \{a, b\}$ and consider the language L over Σ defined by the given regular expression.

a. The regular expression is $a^*b(a \mid b)^*$. Write five strings that belong to L.

b. The regular expression is $a^* \mid (ab)^*$. Indicate which of the following strings belong to L:

$$a \quad b \quad aaaa \quad abba \quad ababab$$

Solution

a. The strings *b*, *ab*, *abbb*, *abaaa*, and *ababba* are five strings from the infinitely many in L.

b. The following strings are the only ones listed that belong to L: *a*, *aaaa*, and *ababab*. The string *b* does not belong to L because it is neither a string of *a*'s nor a string of possibly repeated *ab*'s. The string *abba* does not belong to L because any two *b*'s that might occur in a string of L are separated by an *a*. ■

Example 12.1.9 **A Regular Expression That Defines a Language**

Let $\Sigma = \{0, 1\}$. Find regular expressions over Σ that define the following languages:

a. The language consisting of all strings of 0's and 1's that have even length and in which the 0's and 1's alternate.

b. The language consisting of all strings of 0's and 1's with an even number of 1's. Such strings are said to have *even parity*.

c. The language consisting of all strings of 0's and 1's that do not contain two consecutive 1's.

Solution

a. If a string in the language starts with a 1, the pattern 10 must continue for the length of the string. If it starts with 0, the pattern 01 must continue for the length of the string. Also, the null string satisfies the condition by default. Thus an answer is

$$(10)^* \mid (01)^*.$$

b. Some basic strings with even parity are λ, 0, and 10^*1. Concatenation of strings with even parity also have even parity. Because such a string may start or end with a string of 0's, one answer is

$$(0 \mid 10^*1)^*.$$

c. Note that a string may end in a 1, but any other 1 must be followed immediately by a 0. Thus, it is enough to enforce the rule that a 1 must be followed by a 0, unless the 1 is at the end of the string. A regular expression satisfying these conditions is

$$(0 \mid 10)^*(\lambda \mid 1).$$ ■

Note that a given language may be defined by more than one regular expression. For example, both

$$(a^* \mid b^*)^* \quad \text{and} \quad (a \mid b)^*$$

define the language consisting of the set of all strings of *a*'s and *b*'s.

Example 12.1.10 **Deciding Whether Regular Expressions Define the Same Language**

In (a) and (b), determine whether the given regular expressions define the same language. If they do, describe the language. If they do not, give an example of a string that is in one of the languages but not the other.

a. $(a \mid \lambda)^*$ and a^*

b. $0^* \mid 1^*$ and $(01)^*$

Solution

a. Note that because the null string λ has no characters, when it is concatenated with any other string x, the result is just x: for every string x, $x\lambda = \lambda x = x$. Now $L((a \mid \lambda)^*)$ is the set of strings formed using a and λ in any order, and so, because $a\lambda = \lambda a = a$, this is the same as the set of strings consisting of zero or more a's. Thus $L((a \mid \lambda)^*) = L(a^*)$.

b. The two languages defined by the given regular expressions are not the same: 0101 is in the second language but not the first. ■

Practical Uses of Regular Expressions

Many applications of computers involve performing operations on pieces of text. For instance, word and text processing programs allow us to find certain words or phrases in a document and possibly replace them with others. A compiler for a computer language analyzes an incoming stream of characters to find groupings that represent aspects of the computer language such as keywords, constants, identifiers, and operators. And in bioinformatics, pattern matching and flexible searching techniques are used extensively to analyze the long sequences of the base pairs A, C, G, and T that occur in DNA.

Through their connection with finite-state automata, which we discuss in the next section, regular expressions provide an extremely useful way to describe a pattern in order to identify a string or a collection of strings within a piece of text. Regular expressions make it possible to replace a long, complicated set of if-then-else statements with code that is easy both to produce and to understand. Because of their convenience, regular expressions were introduced into a number of UNIX utilities, such as *grep* (short for ***g***lobally ***s***earch for ***r***egular ***e***xpression and ***p***rint) and *egrep* (***e****xtended grep*), in text editors, such as *QED* (short for ***Q***uick ***ED***itor, the first text editor to use regular expressions), *vi* (short for ***v***isual ***i***nterface), *sed* (short for ***s***tream ***ed***itor and originally developed for UNIX but now used by many systems), and *Emacs* (short for ***E***ditor ***mac***ros), and in the lexical scanner component of a compiler. The computer language Perl has a particularly powerful implementation for regular expressions, which has become a de facto standard. The implementations used in Java, Python, and .NET are similar.

A number of shorthand notations have been developed to facilitate working with regular expressions in text processing. When characters in an alphabet or in a part of an alphabet are understood to occur in a standard order, the notation *[beginning character – ending character]* is commonly used to represent the regular expression that consists of a single character in the range from the beginning to the ending character. It is called a **character class**. Thus

$$[A - C] \quad \text{stands for} \quad (A \mid B \mid C)$$

and

$$[0 - 9] \quad \text{stands for} \quad (0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9).$$

Character classes are also allowed to include more than one range of characters. For instance,

$$[A - C\, x - z] \quad \text{stands for} \quad (A \mid B \mid C \mid x \mid y \mid z)$$

As an example, consider the language defined by the regular expression

$$[A-Z\,a-z]([A-Z\,a-z]\mid[0-9])^*.$$

The following are some strings in the language:

$$\textit{Account Number}, \quad z23, \quad \textit{jsmith}109, \quad \textit{Draft}2\textit{rev}.$$

In general, the language is the set of all strings that start with a letter sequence of digits or letters. This set is the same as the set of allowable number of computer languages.

Other commonly used shorthands are

$$[ABC] \text{ to stand for } (A \mid B \mid C)$$

and a single dot

$$. \text{ to stand for an arbitrary character.}$$

Thus, for instance, if $\Sigma = \{A, B, C\}$, then

$$A.C \quad \text{stands for} \quad (AAC \mid ABC \mid ACC).$$

When the symbol ^ is placed at the beginning of a character class, it indicates that a character of the same type as those in the range of the class is to occur at that point in the string, except for one of the specific characters indicated after the ^ sign. For instance,

$$[\hat{}\,D-Z][0-9][0-9]^*$$

stands for any string starting with a letter of the alphabet different from D to Z, followed by any positive number of digits from 0 to 9. Examples are $B3097$, $C0046$, and so forth. If r is a regular expression, the notation $r+$ denotes the concatenation of r with itself any positive finite number of times. In symbols,

$$r+ = rr^*.$$

For example,

$$[A-Z]+$$

represents any nonempty string of capital letters. If r is a regular expression, then

$$r? = (\lambda \mid r).$$

That is, $r?$ denotes either zero occurrences or exactly one occurrence of r. Finally, if m and n are positive integers with $m \leq n$,

$$r\{n\} \quad \text{denotes the concatenation of } r \text{ with itself exactly } n \text{ times,}$$

and

$$r\{m, n\} \quad \text{denotes the concatenation of } r \text{ with itself anywhere from } m \text{ through } n \text{ times.}$$

Thus a check to help determine whether a given string could represent a local telephone number in the United States is to see whether it has the form

$$[0-9][0-9][0-9]\text{-}[0-9][0-9][0-9][0-9],$$

or, equivalently, whether it has the form

$$[0-9]\{3\}\text{-}[0-9]\{4\}.$$

Example 12.1.11 **A Regular Expression for a Date**

People often write dates in a variety of formats. For instance, in the United States the following all represent the fifth of February of 2050:

$$2/5/2050 \quad 2\text{-}5\text{-}2050 \quad 02/05/2050 \quad 02\text{-}05\text{-}2050$$

Note In most of the rest of the world these expressions represent the second of May of 2050.

Write a regular expression that would help check whether a given string might be a valid date written in one of these forms.

Solution The language defined by the following regular expression consists of all strings that begin with one or two digits followed by either a hyphen or a slash, followed by either one or two digits, followed by either a hyphen or a slash, followed by four digits.

$$[0-9]\{1, 2\}[\text{-}/][0-9]\{1, 2\}[0-9]\{4\}$$

All valid dates of the given format are elements of the language defined by this expression, but the language also includes strings that are not valid dates. For instance, 09/54/1978 is in the language, but it is not a valid date because September does not have 54 days, and 38/12/2184 is not valid because there is no 38th month. It is possible to write a more complicated regular expression that could be used to check all aspects of the validity of a date (see exercise 40 at the end of the section), but the kind of simpler expression given above is nonetheless useful. For instance, it provides an easy way to notify a user of an interactive program that a certain kind of mistake was made and that information should be reentered. ■

TEST YOURSELF

Answers to Test Yourself questions are located at the end of each section.

1. If x and y are strings, the concatenation of x and y is _____.
2. If L and L' are languages, the concatenation of L and L' is _____.
3. If L and L' are languages, the union of L and L' is _____.
4. If L is a language, the Kleene closure of L is _____.
5. The set of regular expressions over an alphabet Σ is defined recursively. The base for the definition is the statement that _____. The recursion for the definition specifies that if r and s are any regular expressions over Σ, then the following are also regular expressions in the set: _____, _____, and _____.
6. The function that associates a language to each regular expression over an alphabet Σ is defined recursively. The base for the definition is the statement that $L(\varnothing)$ = _____, $L(\lambda)$ = _____, and $L(a)$ = _____ for every a in Σ. The recursion for the definition specifies that if $L(r)$ and $L(r')$ are the languages defined by the regular expressions r and r' over Σ, then $L(rr')$ = _____, $L(r \mid r')$ = _____, and $L(r^*)$ = _____.
7. The notation [A − C] is an example of a _____ and denotes the regular expression _____.
8. Use of a single dot in a regular expression stands for _____.
9. The symbol ^, placed at the beginning of a character class, indicates _____.

10. If r is a regular expression, the notation $r+$ denotes _____.

11. If r is a regular expression, the notation $r?$ denotes _____.

12. If r is a regular expression, the notation $r\{n\}$ denotes _____ and the notation $r\{m, n\}$ denotes _____.

EXERCISE SET 12.1*

In 1 and 2, let $\Sigma = \{x, y\}$ be an alphabet.

1. a. Let L_1 be the language consisting of all strings over Σ that are palindromes and have length ≤ 4. List the elements of L_1 between braces.

b. Let L_2 be the language consisting of all strings over Σ that begin with an x and have length ≤ 3. List the elements of L_2.

2. a. Let L_3 be the language consisting of all strings over Σ of length ≤ 3 in which all the x's appear to the left of all the y's. List the elements of L_3 between braces.

b. List between braces the elements of Σ^4, the set of all strings of length 4 over Σ.

c. Let $A = \Sigma^1 \cup \Sigma^1$ and $B = \Sigma^3 \cup \Sigma^4$. Describe A, B, and $A \cup B$ in words.

3. a. If the expression $ab + cd +\cdot$ in postfix notation is converted to infix notation, what is the result?

***H* b.** Let $\Sigma = \{1, 2, *, /\}$ and let L be the set of all strings over Σ obtained by writing first a number (1 or 2), then a second number (1 or 2), which can be the same as the first one, and finally an operation (denoted $*$ or $/$, where $*$ indicates multiplication and $/$ indicates division). Then L is a set of postfix, or reverse Polish, expressions. List all the elements of L between braces, and evaluate the resulting expressions.

In 4–6, describe L_1L_2, $L_1 \cup L_2$, and $(L_1 \cup L_2)^*$ for the given languages L_1 and L_2.

4. L_1 is the set of all strings of a's and b's that start with an a and contain only that one a; L_2 is the set of all strings of a's and b's that contain an even number of a's.

5. L_1 is the set of all strings of a's, b's, and c's that contain no c's and have the same number of a's as b's; L_2 is the set of all strings of a's, b's, and c's that contain no a's or b's.

6. L_1 is the set of all strings of 0's and 1's that start with a 0; L_2 is the set of all strings of 0's and 1's that end with a 0.

In 7–9, add parentheses to emphasize the order of precedence in the given expressions.

7. $(a \mid b^*b)(a^* \mid ab)$ **8.** $0^*1 \mid 0(0^*1)^*$

9. $(x \mid yz^*)^*(yx \mid (yz)^*z)$

In 10–12, use the rules about order of precedence to eliminate the parentheses in the given regular expression.

10. $((a(b^*)) \mid (c(b^*)))\ ((ac) \mid (bc))$

11. $(1(1^*)) \mid ((1(0^*)) \mid ((1^*)1))$

12. $(xy)(((x^*)y)^*) \mid (((yx) \mid y)(y^*))$

In 13–15, use set notation to derive the language defined by the given regular expression. Assume $\Sigma = \{a, b, c\}$.

13. $\lambda \mid ab$ **14.** $\varnothing \mid \lambda$ **15.** $(a \mid b)c$

In 16–18, write five strings that belong to the language defined by the given regular expression.

16. $0^*1(0^*1^*)^*$ **17.** $b^* \mid b^*ab^*$ **18.** $x^*(yxxy \mid x)^*$

In 19–21, use words to describe the language defined by the given regular expression.

19. $b^*ab^*ab^*a$ **20.** $1(0 \mid 1)^*00$ **21.** $(x \mid y)y(x \mid y)^*$

In 22–24, indicate whether the given strings belong to the language defined by the given regular expression. Briefly justify your answers.

22. Expression: $(b \mid \lambda)a(a \mid b)^*a(b \mid \lambda)$, strings: *aaaba*, *baabb*

23. Expression: $(x^*y \mid zy^*)^*$, strings: *zyyxz*, *zyyzy*

24. Expression: $(01^*2)^*$, strings: 120, 01202

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol ***H*** indicates that only a hint or a partial solution is given. The symbol * signals that an exercise is more challenging than usual.

In 25–27, find a regular expression that defines the given language.

25. The language consisting of all strings of 0's and 1's with an odd number of 1's. (Such a string is said to have *odd parity*.)

26. The language consisting of all strings of a's and b's in which the third character from the end is a b.

27. The language consisting of strings of x's and y's in which the elements in every pair of x's are separated by at least one y.

Let r, s, and t be regular expressions over $\Sigma = \{a, b\}$. In 28–30, determine whether the two regular expressions define the same language. If they do, describe the language. If they do not, give an example of a string that is in one of the languages but not the other.

28. $(r \mid s)t$ and $rt \mid st$

29. $(rs)^*$ and r^*s^*

30. $(rs)^*$ and $((rs)^*)^*$

In 31–39, write a regular expression to define the given set of strings. Use the shorthand notations given in the section whenever convenient. In most cases, your expression will describe other strings in addition to the given ones, but try to make your answer fit the given strings as closely as possible within reasonable space limitations.

31. All words that are written in lowercase letters and start with the letters *pre* but do not consist of *pre* all by itself.

32. All words that are written in uppercase letters, and contain the letters *BIO* (as a unit) or *INFO* (as a unit).

33. All words that are written in lowercase letters, end in *ly*, and contain at least five letters.

34. All words that are written in lowercase letters and contain at least one of the vowels a, e, i, o, or u.

35. All words that are written in lowercase letters and contain exactly one of the vowels a, e, i, o, or u.

36. All words that are written in uppercase letters and do not start with one of the vowels A, E, I, O, or U but contain exactly two of these vowels next to each other.

37. All United States social security numbers (which consist of three digits, a hyphen, two digits, another hyphen, and finally four more digits), where the final four digits start with a 3 and end with a 6.

38. All telephone numbers that have three digits, then a hyphen, then three more digits, then a hyphen, and then four digits, where the first three digits are either 800 or 888 and the last four digits start and end with a 2.

39. All signed or unsigned numbers with or without a decimal point. A signed number has one of the prefixes + or −, and an unsigned number does not have a prefix. Represent the decimal point as \. to distinguish it from the single dot symbol for an arbitrary character.

***H* 40.** Write a regular expression to perform a complete check to determine whether a given string represents a valid date from 1980 to 2079 written in one of the formats of Example 12.1.11. (During this period, leap years occur every four years starting in 1980.)

*** 41.** Write a regular expression to define the set of strings of 0's and 1's with an even number of 0's and even number of 1's.

ANSWERS FOR TEST YOURSELF

1. the string obtained by writing all the characters of x followed by all the characters of y **2.** $\{xy \mid x \in L$ and $y \in L'\}$ **3.** $\{s \mid s \in L$ or $s \in L'\}$ **4.** $\{t \mid t$ is a concatenation of any finite number of strings in $L\}$ **5.** $\varnothing$, λ, and each individual symbol in Σ are regular expressions over Σ; (rs); $(r \mid s)$; (r^*) **6.** $\varnothing$; $\{\lambda\}$; $\{a\}$; $L(r)L(r')$; $L(r) \cup L(r')$; $(L(r))^*$ **7.** character class; $(A \mid B \mid C)$ **8.** an arbitrary character **9.** a character of the same type as those in the range of the class is to occur at that point in the string except for one of the specific characters indicated after the ^ sign. **10.** the concatenation of r with itself any positive finite number of times **11.** $(\lambda \mid r)$ **12.** the concatenation of r with itself exactly n times; the concatenation of r with itself anywhere from m through n times

12.2 Finite-State Automata

The world of the future will be an ever more demanding struggle against the limitations of our intelligence, not a comfortable hammock in which we can lie down to be waited upon by our robot slaves. —Norbert Wiener, 1964

The kind of circuit discussed in Section 2.4 is called a *combinational circuit*. Such a circuit is characterized by the fact that its output is completely determined by its input/output table, or, in other words, by a Boolean function. Its output does not depend in any way on the history of previous inputs to the circuit. For this reason, a combinational circuit is said to have no memory.

Combinational circuits are very important in computer design, but they are not the only type of circuits used. Equally important are *sequential circuits*. For sequential circuits one cannot predict the output corresponding to a particular input unless one also knows something about the prior history of the circuit, or, more technically, unless one knows the state the circuit was in before receiving the input. The behavior of a sequential circuit is a function not only of the input to the circuit but also of the state the circuit is in when the input is received. A computer memory circuit is a type of sequential circuit.

A **finite-state automaton** is an idealized machine that embodies the essential idea of a sequential circuit. Each piece of input to a finite-state automaton leads to a change in the state of the automaton, which in turn affects how subsequent input is processed. Imagine, for example, the act of dialing a telephone number. Dialing 1-800 puts the telephone circuit in a state of readiness to receive the final seven digits of a toll-free call, whereas dialing 328 leads to a state of expectation for the four digits of a local call. Vending machines operate similarly. Just knowing that you put a quarter into a vending machine is not enough for you to be able to predict what the behavior of the machine will be. You also have to know the state the machine was in when the quarter was inserted. If 75¢ had already been deposited, you might get a beverage or some candy, but if the quarter was the first coin deposited, you would probably get nothing at all.

Example 12.2.1 A Simple Vending Machine

A simple vending machine dispenses bottles of juice that cost $1 each. The machine accepts quarters and half-dollars only and does not give change. As soon as the amount deposited equals or exceeds $1 the machine releases a bottle of juice. The next coin deposited starts the process over again. The operation of the machine is represented by the diagram of Figure 12.2.1.

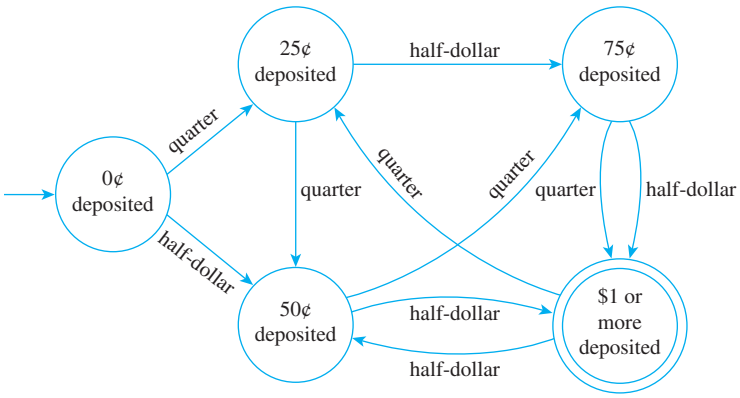


FIGURE 12.2.1 A Simple Vending Machine

Each circle represents a state of the machine: the state in which 0¢ has been deposited, 25¢, 50¢, 75¢, and $1 or more. The unlabeled arrow pointing to "0¢ deposited" indicates that this is the initial state of the machine. The double circle around "$1 or more deposited" indicates that a bottle of juice is released when the machine has reached this state. (It is called an *accepting state* of the machine because when the machine is in this state, it has accepted the input sequence of coins as payment for juice.) The arrows that link the states indicate what happens when a particular input is made to the machine in each of its various states. For instance, the arrow labeled "quarter" that goes from "0¢ deposited" to "25¢ deposited" indicates that when the machine is in the state "0¢ deposited" and a quarter is inserted, the machine goes to the state "25¢ deposited." The arrow labeled "half-dollar" that goes from "75¢ deposited" to "$1 or more deposited" indicates that when the machine is in the state "75¢ deposited" and a half-dollar is inserted, the machine goes to the state "$1 or more deposited" and juice is dispensed. (In this case the purchaser would pay $1.25 for the juice because the machine does not return change.) The arrow labeled "quarter" that goes from "$1 or more deposited" to "25¢ deposited" indicates that when the machine is in the state "$1 or more deposited" and a quarter is inserted, the machine goes back to the state "25¢ deposited." (This corresponds to the fact that after the machine has dispensed a bottle of juice, it starts operation all over again.)

Equivalently, the operation of the vending machine can be represented by a *next-state table* as shown in Table 12.2.1.

TABLE 12.2.1 Next-State Table

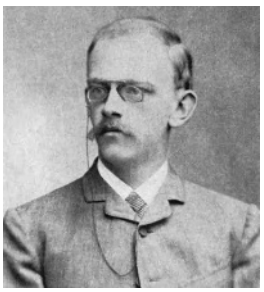
		Input	
		Quarter	**Half-Dollar**
→	0¢ deposited	25¢ deposited	50¢ deposited
	25¢ deposited	50¢ deposited	75¢ deposited
State	50¢ deposited	75¢ deposited	$1 or more deposited
	75¢ deposited	$1 or more deposited	$1 or more deposited
◎	$1 or more deposited	25¢ deposited	50¢ deposited

The entries in the left-most column are all the possible states of the machine, with the arrow pointing to "0¢ deposited" indicating that the machine begins operation in this state and the double circle next to "$1 or more deposited" showing that a bottle of juice is released when the machine has reached this state. The inputs to the machine are shown in at the tops of the columns labeled "Quarter" and "Half-Dollar." Entries in the body of the table show the states to which the machine goes when it has been in one state and a given input is applied to it. For instance, the entry in the third row of the column labeled "Half-Dollar" shows that when the machine is in state "50¢ deposited" and a half-dollar is deposited, it goes to state "$1 or more deposited."

Note that Table 12.2.1 conveys exactly the same information as the diagram of Figure 12.2.1. If the diagram is given, the table can be constructed, and if the table is given, the diagram can be drawn. ■

Observe that the vending machine described in Example 12.2.1 can be thought of as having a primitive memory: It "remembers" how much money has been deposited (within limits) by referring to the state it is in. This capability for storing information and acting upon it is what gives finite-state automata their tremendous power.

The most important finite-state automata are digital computers. Each computer consists of several subsystems: input devices, a processor, and output devices. A processor typically consists of a central processing unit and a finite number of memory locations. At any given



Paul Fearn/Alamy Stock Photo

David Hilbert
(1862–1943)

time, the state of the processor is determined by the locations and values of all the bits stored within its memory. A computer that has n different locations for storing a single bit can therefore exist in 2^n different states. For a modern computer, n is many billions or even trillions, so the total number of states is enormous. But it *is* finite. Therefore, despite the complexity of a computer, just as for a vending machine, it is possible to predict the next state given knowledge of the current state and the input. Indeed, this is essentially what programmers try to do every time they write a program. Fortunately, modern, high-level computer languages provide a lot of help.

The basic theory of automata was developed to answer very theoretical questions about the foundations of mathematics posed by the great German mathematician David Hillbert in 1900. The ground-breaking work on automata was done in the mid-1930s by the English mathematician and logician Alan Turing. In the 1940s and 1950s, Turing's work played an important role in the development of real-world automatic computers.

Science History Images/Alamy Stock Photo

Alan M. Turing
(1912–1954)

Definition of a Finite-State Automaton

A general *finite-state automaton* is completely described by giving a set of states, together with an indication about which is the initial state and which are the accepting states (when something special happens), a list of all input elements, and specification for a *next-state function* that defines which state is produced by each input in each state. This is formalized in the following definition:

Definition

A **finite-state automaton** A consists of five objects:

1. A finite set I, called the **input alphabet**, of input symbols.
2. A finite set S of **states** the automaton can assume.
3. A designated state s_0 called the **initial state**.
4. A designated set of states called the set of **accepting states**.
5. A **next-state function** $N: S \times I \to S$ that associates a "next-state" to each ordered pair consisting of a "current state" and a "current input." For each state s in S and input symbol m in I, $N(s, m)$ is the state to which A goes if m is input to A when A is in state s.

The operation of a finite-state automaton is commonly described by a diagram called a **(state-) transition diagram**, similar to that of Figure 12.2.1. It is called a *transition diagram* because it shows the transitions the machine makes from one state to another in response to various inputs. In a transition diagram, states are represented by circles and accepting states by double circles. There is one arrow that points to the initial state and there are other arrows that are labeled with input symbols and point from each state to other states to indicate the action of the next-state function. Specifically, an arrow from state s to state t labeled m means that $N(s, m) = t$.

The **next-state table** for an automaton shows the values of the next-state function N for all possible states s and input symbols i. In the **annotated next-state table**, the initial state is indicated by an arrow and the accepting states are marked by double circles.

Example 12.2.2 **A Finite-State Automaton Given by a Transition Diagram**

Consider the finite-state automaton A defined by the transition diagram shown in Figure 12.2.2.

a. What are the states of A?
b. What are the input symbols of A?
c. What is the initial state of A?
d. What are the accepting states of A?
e. Determine $N(s_1, 1)$.
f. Construct the annotated next-state table for A.

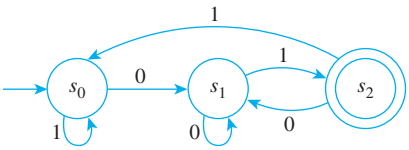


FIGURE 12.2.2

Solution

a. The states of A are s_0, s_1, and s_2 *[since these are the labels of the circles]*.
b. The input symbols of A are 0 and 1 *[since these are the labels of the arrows]*.
c. The initial state of A is s_0 *[since the unlabeled arrow points to s_0]*.
d. The only accepting state of A is s_2 *[since this is the only state marked by a double circle]*.
e. $N(s_1, 1) = s_2$ *[since there is an arrow from s_1 to s_2 labeled 1]*
f.

State		Input 0	1
→	s_0	s_1	s_0
	s_1	s_1	s_2
◎	s_2	s_1	s_0

■

Example 12.2.3 **A Finite-State Automaton Given by an Annotated Next-State Table**

Consider the finite-state automaton A defined by the following annotated next-state table:

a. What are the states of A?
b. What are the input symbols of A?
c. What is the initial state of A?
d. What are the accepting states of A?
e. Find $N(U, c)$.
f. Draw the transition diagram for A.

State		Input a	b	c
→	U	Z	Y	Y
◎	V	V	V	V
	Y	Z	V	Y
◎	Z	Z	Z	Z

Solution

a. The states of A are U, V, Y, and Z.
b. The input symbols of A are a, b, and c.
c. The initial state of A is U *[since the arrow points to U]*.
d. The accepting states of A are V and Z *[since these are marked with double circles]*.
e. $N(U, c) = Y$ *[since the entry in the row labeled U and the column labeled c of the next-state table is Y]*.
f. The transition diagram for A is shown in Figure 12.2.3. It can be drawn more compactly by labeling arrows with multiple-input symbols where appropriate. This is illustrated in Figure 12.2.4.

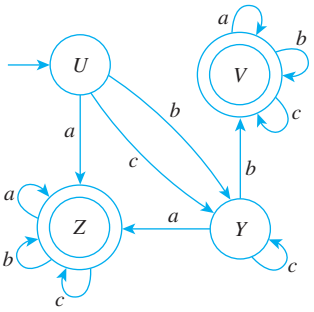


FIGURE 12.2.3

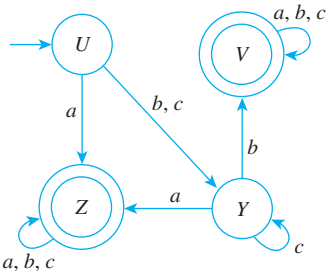


FIGURE 12.2.4 ■

The Language Accepted by an Automaton

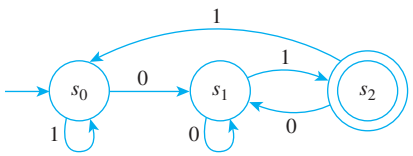
Now suppose a string of input symbols is fed into a finite-state automaton in sequence. At the end of the process, after each successive input symbol has changed the state of the automaton, the automaton ends up in a certain state, which may be either an accepting state or a nonaccepting state. In this way, the action of a finite-state automaton separates the set of all strings of input symbols into two subsets: those that send the automaton to an accepting state and those that do not. Those strings that send the automaton to an accepting state are said to be *accepted* by the automaton.

Definition

Let A be a finite-state automaton with set of input symbols I. Let I^* be the set of all strings over I, and let w be a string in I^*. Then ***w* is accepted by *A*** if, and only if, A goes to an accepting state when the symbols of w are input to A in sequence from left to right, starting when A is in its initial state. The **language accepted by *A***, denoted ***L*(*A*)**, is the set of all strings that are accepted by A.

Example 12.2.4 **Finding the Language Accepted by an Automaton**

Consider the finite-state automaton A defined in Example 12.2.2 and shown again below.



a. To what states does A go if the symbols of the following strings are input to A in sequence, starting from the initial state?

(i) 01 (ii) 0011 (iii) 0101100 (iv) 10101

b. Which of the strings in part (a) send A to an accepting state?

c. What is the language accepted by A?

d. Is there a regular expression that defines the same language?

Solution

a. (i) s_2 (ii) s_0 (iii) s_1 (iv) s_2

b. The strings 01 and 10101 send A to an accepting state.

c. Observe that if w is any string that ends in 01, then w is accepted by A. For if w is any string of length $n \geq 2$, then after the first $n - 2$ symbols of w have been input, A is in one of its three states: s_0, s_1, or s_2. But from any of these three states, input of the symbols 01 in sequence sends A first to s_1 and then to the accepting state s_2. Hence any string that ends in 01 is accepted by A.

Also note that the only strings accepted by A are those that end in 01. (That is, no other strings besides those ending in 01 are accepted by A.) The reason is that the only accepting state of A is s_2, and the only arrow pointing to s_2 comes from s_1 and is labeled 1. Thus in order for an input string w of length n to send A to an accepting state, the last symbol of w must be a 1 and the first $n - 1$ symbols of w must send A to state s_1. Now three arrows point to s_1, one from each of the three states of A, and all are labeled 0. Thus the last of the first $n - 1$ symbols of w must be 0, or, in other words, the next-to-the-last symbol of w must be 0. Hence the last two symbols of w must be 01, and thus

$$L(A) = \text{the set of all strings of 0's and 1's that end in 01.}$$

d. Yes. One regular expression that defines $L(A)$ is $(0 \mid 1)^*01$. ■

A finite-state automaton with multiple accepting states can have output devices attached to each one so that the automaton can classify input strings into a variety of different categories, one for each accepting state. This is how finite-state automata are used in the lexical scanner component of a computer compiler to group the symbols from a stream of input characters into identifiers, keywords, and so forth.

The Eventual-State Function

Now suppose a finite-state automaton is in one of its states (not necessarily the initial state) and a string of input symbols is fed into it in sequence. To what state will the automaton eventually go? The function that gives the answer to this question for every possible combination of input strings and states of the automaton is called the *eventual-state function*.

Definition

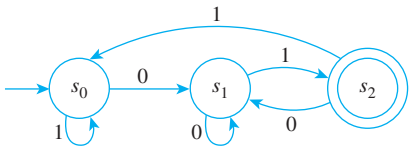
Let A be a finite-state automaton with set of input symbols I, set of states S, and next-state function $N: S \times I \to S$. Let I^* be the set of all strings over I, and define the **eventual-state function** $N^*: S \times I^* \to S$ as follows:

For any state s and for any input string w,

$$N^*(s, w) = \left[\begin{array}{l}\text{the state to which } A \text{ goes if the} \\ \text{symbols of } w \text{ are input to } A \text{ in sequence,} \\ \text{starting when } A \text{ is in state } s\end{array}\right].$$

Example 12.2.5 **Computing Values of the Eventual-State Function**

Consider again the finite-state automaton of Example 12.2.2 shown below for convenience. Find $N^*(s_1, 10110)$.



Solution By definition of the eventual-state function,

$$N^*(s_1, 10110) = \begin{bmatrix} \text{the state to which } A \text{ goes if the} \\ \text{symbols of 10110 are input to } A \text{ in} \\ \text{sequence, starting when } A \text{ is in state } s_1 \end{bmatrix}.$$

By referring to the transition diagram for A, you can see that starting from s_1, when a 1 is input, A goes to s_2; then when a 0 is input, A goes back to s_1; after that, when a 1 is input, A goes to s_2; from there, when a 1 is input, A goes to s_0; and finally, when a 0 is input, A goes back to s_1. This sequence of state transitions can be written as follows:

$$s_1 \xrightarrow{1} s_2 \xrightarrow{0} s_1 \xrightarrow{1} s_2 \xrightarrow{1} s_0 \xrightarrow{0} s_1.$$

Thus, after all the symbols of 10110 have been input in sequence, the eventual state of A is s_1, so

$$N^*(s_1, 10110) = s_1.$$ ■

The definitions of string and language accepted by an automaton can be restated symbolically using the eventual-state function. Suppose A is a finite-state automaton with set of input symbols I and next-state function N, and suppose that I^* is the set of all strings over I and that w is a string in I^*.

$$w \text{ is accepted by } A \iff N^*(s_0, w) \text{ is an accepting state of } A$$

$$L(A) = \{w \in I^* \mid N^*(s_0, w) \text{ is an accepting state of } A\}$$

Designing a Finite-State Automaton

Now consider the problem of starting with a description of a language and designing an automaton to accept exactly that language.

Example 12.2.6 **A Finite-State Automaton That Accepts the Set of Strings of 0's and 1's for Which the Number of 1's Is Divisible by 3**

a. Design a finite-state automaton A that accepts the set of all strings of 0's and 1's such that the number of 1's in the string is divisible by 3.

b. Is there a regular expression that defines this set?

Solution

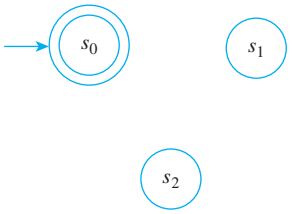
a. Let s_0 be the initial state of A, s_1 its state after one 1 has been input, and s_2 its state after two 1's have been input. Note that s_0 is the state of A after zero 1's have been input, and since zero is divisible by 3 ($0 = 0 \cdot 3$), s_0 must be an accepting state.

The states s_0, s_1, and s_2 must be different from one another because from state s_0 three 1's are needed to reach a new total divisible by 3, whereas from state s_1 two additional 1's are necessary, and from state s_2 just one more 1 is required.

Now the state of A after three 1's have been input can also be taken to be s_0 because after three 1's have been input, three more are needed to reach a new total divisible by 3. More generally, if $3k$ 1's have been input to A, where k is any nonnegative integer, then three more are needed for the total again to be divisible by 3 (since $3k + 3 = 3(k + 1)$). Thus the state in which $3k$ 1's have been input, for any nonnegative integer k, can be taken to be the initial state s_0.

By similar reasoning, the states in which $(3k + 1)$ 1's and $(3k + 2)$ 1's have been input, where k is a nonnegative integer, can be taken to be s_1 and s_2, respectively.

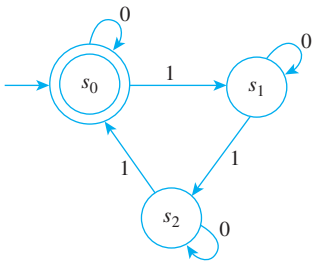
Now every nonnegative integer can be written in one of the three forms $3k$, $3k + 1$, or $3k + 2$ (see Section 4.5), so the three states s_0, s_1, and s_2 are all that is needed to create A. Thus the states of A can be drawn and labeled as shown below.



Next consider the possible inputs to A in each of its states. No matter what state A is in, if a 0 is input the total number of 1's in the input string remains unchanged. Thus there is a loop at each state labeled 0.

Now suppose a 1 is input to A when it is in state s_0. Then A goes to state s_1 (since the total number of 1's in the input string has changed from $3k$ to $3k + 1$). Similarly, if a 1 is input to A when it is in state s_1, then A goes to state s_2 (since the total number of 1's in the input string has changed from $3k + 1$ to $3k + 2$). Finally, if a 1 is input to A when it is in state s_2, then it goes to state s_0 (since the total number of 1's in the input string becomes $(3k + 2) + 1 = 3k + 3 = 3(k + 1)$, which is a multiple of 3).

It follows that the transition diagram for A has the appearance shown below.



This automaton accepts the set of strings of 0's and 1's for which the number of 1's is divisible by 3.

b. A regular expression that defines the given set is $0^*|(0^*10^*\ 10^*10^*)^*$. ■

Example 12.2.7 **A Finite-State Automaton That Accepts the Set of All Strings of 0's and 1's Containing Exactly One 1**

a. Design a finite-state automaton A to accept the set of all strings of 0's and 1's that contain exactly one 1.

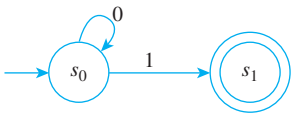
b. Is there a regular expression that defines this set?

Solution

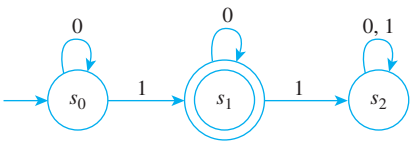
a. The automaton A must have at least two distinct states:

s_0: initial state;
s_1: state to which A goes when the input string contains exactly one 1.

If A is in state s_0 and a 0 is input, A may as well stay in state s_0 (since it still needs to wait for a 1 to move to state s_1), but as soon as a 1 is input, A moves to state s_1. Thus a partial drawing of the transition diagram is as shown below.



Now consider what happens when A is in state s_1. If a 0 is input, the input string still has a single 1, so A stays in state s_1. But if a 1 is input, then the input string contains more than one 1, so A must leave s_1 (since no string with more than one 1 is to be accepted by A). It cannot go back to state s_0 because there is a way to get from s_0 to s_1, and after input of the second 1, A can never return to state s_1. Hence A must go to a third state, s_2, from which there is no return to s_1. Thus from s_2 every input may as well leave A in state s_2. It follows that the completed transition diagram for A has the appearance shown below.

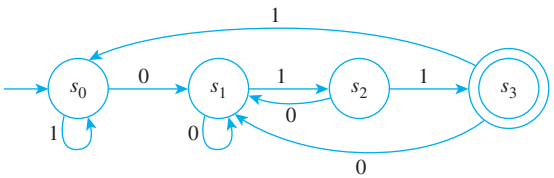


This automaton accepts the set of strings 0's and 1's, with exactly one 1.

b. A regular expression that defines the given set is 0^*10^*. ■

Simulating a Finite-State Automaton Using Software

Suppose items have been coded with strings of 0's and 1's. A program is to be written to govern the processing of items coded with strings that end in 011; items coded any other way are to be ignored. This situation can be modeled by the finite-state automaton shown in Figure 12.2.5.



This automaton recognizes strings that end in 011.

FIGURE 12.2.5

The symbols of the code for the item are fed into this automaton in sequence, and every string of symbols in a given code sends the automaton to one of the four states s_0, s_1, s_2, or s_3. If state s_3 is reached, the item is processed; if not, the item is ignored.

The action of this finite-state automaton can be simulated by a computer algorithm as given in Algorithm 12.2.1.

Algorithm 12.2.1 A Finite-State Automaton

[This algorithm simulates the action of the finite-state automaton of Figure 12.2.5 by mimicking the functioning of the transition diagram. The states are denoted 0, 1, 2, *and* 3.*]*

Input: string *[a string of* 0*'s and* 1*'s plus an end marker e]*

Algorithm Body:

```
state := 0
symbol := first symbol in the input string
while (symbol ≠ e)
   if   state = 0   then if symbol = 0
                         then state := 1
                         else state = 0
   else if state = 1 then if symbol = 0
                         then state := 1
                         else state := 2
   else if state = 2 then if symbol = 0
                         then state := 1
                         else state := 3
   else if state = 3 then if symbol = 0
                         then state := 1
                         else state := 0
   symbol := next symbol in the input string
end while
```

[After execution of the **while** *loop, the value of state is* 3 *if, and only if, the input string ends in* 011*e.]*

Output: *state*

Note how use of the finite-state automaton allows the creator of the algorithm to focus on each step of the analysis of the input string independently of the other steps.

An alternative way to program this automaton is to enter the values of the next-state function directly as a two-dimensional array. This is done in Algorithm 12.2.2.

Algorithm 12.2.2 A Finite-State Automaton

[This algorithm simulates the action of the finite-state automaton of Figure 12.2.5 by repeated application of the next-state function. The states are denoted 0, 1, 2, *and* 3.*]*

Input: *string [a string of* 0*'s and* 1*'s plus an end marker e]*

Algorithm Body:

```
N(0, 0) := 1, N(0, 1) := 0, N(1, 0) := 1, N(1, 1) := 2,
N(2, 0) := 1, N(2, 1) := 3, N(3, 0) := 1, N(3, 1) := 0
state := 0
symbol := first symbol in the input string
```

while (*symbol* ≠ *e*)
  state := *N* (*state, symbol*)
  symbol := next symbol in the input string
end while

[After execution of the **while** *loop, the value of state is* 3 *if, and only if, the input string ends in* 011*e.]*

Output: *state*

Finite-State Automata and Regular Expressions

In the previous sections, each time we considered a language accepted by a finite-state automaton, we found a regular expression that defined the same language. Stephen Kleene showed that our ability to do this is not sheer coincidence. He proved that any language accepted by a finite-state automaton can be defined by a regular expression and that, conversely, any language defined by a regular expression is accepted by a finite-state automaton. Thus for the many applications of regular expressions discussed in Section 12.1, it is theoretically possible to find a corresponding finite-state automaton, which can then be simulated using the kinds of computer algorithms described in the previous subsection.

In practice, it is often of interest to retain only pieces of the patterns sought. For instance, to obtain a reference in an HTML document, one would specify a regular expression defining the full HTML tag, <ahref= "the desired URL">, but one would be interested in retrieving only the string between the quotation marks. Because of these kinds of considerations, actual implementations of finite-state automata include additional features.*

We break the statement of Kleene's theorem into two parts.

Kleene's Theorem, Part 1

Given any language that is accepted by a finite-state automaton, there is a regular expression that defines the same language.

Proof: Suppose A is a finite-state automaton with a set I of input symbols, a set S of n states, and a next-state function N: $S \times I \rightarrow S$. Let I^* denote the set of all strings over I. Number the states $s_1, s_2, s_3, \ldots, s_n$, using s_1 to denote the initial state, and for each integer $k = 1, 2, 3, \ldots, n$, let

$$L_{i,j}^k = \left\{ x \in I^* \;\middle|\; \begin{array}{l} \text{when the symbols of } x \text{ are input to } A \text{ in sequence,} \\ A \text{ goes from state } s_i \text{ to state } s_j \text{ without traveling} \\ \text{through an intermediate state } s_h \text{ for which } h > k \end{array} \right\}.$$

Note that either index i or index j in $L_{i,j}^k$ could be greater than k; the only restriction is that the symbols of a string in $L_{i,j}^k$ cannot make A both enter and exit an intermediate state with index greater than k.

(continued on page 852)

*For more information, see *Mastering Regular Expressions*, 3rd ed., by Jeffrey E. F. Friedl (Sebastopol, CA: O'Reilly & Associates, 2006). Tutorials are also available on the Internet.

If s_j is an accepting state and if $k = n$ and $i = 1$, then $L^n_{1,j}$ is the set of all strings that send A to s_j when the symbols of the string are input to A in sequence starting from s_1. Thus

$$L^n_{1,j} \subseteq L(A).$$

Moreover, because the sequence of symbols in every string in $L(A)$ sends A to *some* accepting state s_j,

$$L(A) \text{ is the union of all the sets } L^n_{1,j}, \text{ where } s_j \text{ is an accepting state.}$$

We use a version of mathematical induction to build up a set of regular expressions over I. Let the property $P(m)$ be the sentence

> For any pair of integers i and j with $1 \le i, j \le n$,
> there is a regular expression $r^m_{i,j}$ that defines $L^m_{i,j}$. ← $P(m)$

Show that P(0) is true: For each pair of integers i and j with $1 \le i, j \le n$, $L^0_{i,j}$ is the set of all strings that send A from s_i to s_j without sending it through any intermediate state s_h for which $h > 0$. Because the subscript of every state in A is greater than zero, the strings in $L^0_{i,j}$ do not send A through any intermediate states at all, and so each is a single input symbol from I. In other words, for all integers i and j with $1 \le i, j \le n$,

$$L^0_{i,j} = \{a \in I \mid N(s_i, a) = s_j\}.$$

Hence $L^0_{i,j}$ is a subset of I, and so (because I is finite), there is an integer M so that we may denote the elements of $L^0_{i,j}$ as follows:

$$L^0_{i,j} = \{a_1, a_2, a_3, \ldots, a_M\} \subseteq I.$$

Now, by definition of regular expression, each single input symbol of I is a regular expression over I; thus every element of $L^0_{i,j}$ is a regular expression over I. The result is that for all integers i and j with $1 \le i, j \le n$, the following regular expression defines $L^0_{i,j}$:

$$a_1 \mid a_2 \mid a_3 \mid \cdots \mid a_M$$

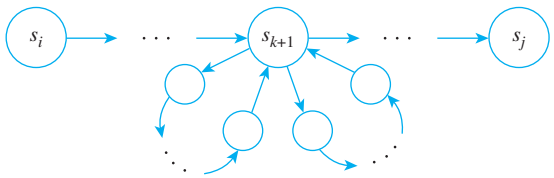
Show that for every integer k with $0 \le k \le n$, if P(k) is true then P(k + 1) is true: Let k be any integer with $1 \le k \le n$, and suppose that

> For each pair of integers p and q with $1 \le p, q \le n$, ← $P(k)$
> there is a regular expression $r^k_{p,q}$ that defines $L^k_{p,q}$. inductive hypothesis

We will show that

> For each pair of integers i and j with $1 \le i, j \le n$,
> there is a regular expression $r^{k+1}_{i,j}$ that defines $L^{k+1}_{i,j}$. ← $P(k+1)$

So suppose that i and j are any pair of integers with $1 \le i, j \le n$, and observe that any string in $L^{k+1}_{i,j}$ sends A from s_i to s_j, either by a route that makes A pass through s_{k+1} or by a route that does not make A pass through s_{k+1}. Now each string that sends A from s_i to s_j and makes A pass through s_{k+1} one or more times can be broken into segments. The symbols in the first segment send A from s_i to s_{k+1} without making A pass through s_{k+1}; those in each of the intermediate segments send s_{k+1} to itself without making A pass through s_{k+1}; and those in the final segment send A from s_{k+1} to s_j without making A pass through s_{k+1}. (The intermediate segment could be the null string.) A typical path showing two intermediate segments is illustrated on the next page.



Note that each intermediate segment of the string is in $L^k_{k+1,\,k+1}$, and by assumption the regular expression $r^k_{k+1,\,k+1}$ defines this set. By the same reasoning, $r^k_{i,\,k+1}$ defines the set of all possible first segments of the string, and $r^k_{k+1,\,j}$ defines the set of all possible final segments of the string. In addition, $r^k_{i,\,j}$ defines the set of all strings that send A from s_i to s_j without making it pass through a state s_m with $m > k$. Thus we may define the regular expression $r^{k+1}_{i,j}$ as follows:

$$r^{k+1}_{i,\,j} = r^k_{i,\,j} \,|\, r^k_{i,\,k+1}(r^k_{k+1,\,k+1})^* r^k_{k+1,\,j}.$$

Then $r^{k+1}_{i,\,j}$ defines the set of all strings that send A from s_i to s_j without making it pass through any states s_m with $m > k+1$, and so $r^{k+1}_{1,\,j}$ defines $L^{k+1}_{1,\,j}$ *[as was to be shown].*

To complete the proof, let $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$ be the accepting state of A. Because $L(A)$ is the union of all the $L^n_{1,\,j}$ where s_j is an accepting state, we have

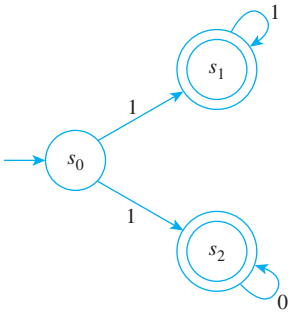
$$\begin{aligned} L(A) &= L\left(r^n_{1,\,j_1}\right) \cup L\left(r^n_{1,\,j_2}\right) \cup \cdots \cup L\left(r^n_{1,\,j_n}\right) \\ &= L\left(r^n_{1,\,j_1} \,|\, r^n_{1,\,j_2}| \cdots |\, r^n_{1,\,j_n}\right) \end{aligned}$$

by the recursive definition for the language defined by a regular expression

Thus if we let $r = r^n_{1,\,j_1} \,|\, r^n_{1,\,j_2}| \cdots |\, r^n_{1,\,j_n}$, we have that $L(A) = L(r)$. In other words, we have constructed a regular expression r that defines the language accepted by A.

Kleene's Theorem, Part 2

Given any language defined by a regular expression, there is a finite-state automaton that accepts the same language.



The most common way to prove part 2 of Kleene's theorem is to introduce a new category of automata called *nondeterministic finite-state automata*. These are similar to the (deterministic) finite-state automata we have been discussing, except that for any given state and input symbol, the next state is a subset of the set of states of the automaton, possibly even the empty set. Thus the next state of the automaton is not uniquely determined by the combination of a current state and an input symbol. A string is accepted by a nondeterministic finite-state automaton if, and only if, when the symbols in the string are input to the automaton in sequence, starting from an initial state, there is *some* sequence of next states through which the automaton could travel that would send it to an accepting state. For instance, the transition diagram at the left is an example of a very simple nondeterministic finite-state automaton that accepts the set of all strings beginning with a 1. Observe that $N(s_0, 1) = \{s_1, s_2\}$ and $N(s_0, 0) = \varnothing$.

Given a language defined by any regular expression, there is a straightforward recursive algorithm for finding a nondeterministic finite-state automaton that defines the same language. The proof of Kleene's theorem is completed by showing that for any such non-deterministic finite-state automaton, there is a (deterministic) finite-state automaton that defines the same language. We leave the details of the proof to a course in automata theory.

Regular Languages

According to Kleene's theorem, the set of languages defined by regular expressions is identical to the set of languages accepted by finite-state automata. Any such language is called a **regular language**. The brief allusions we made earlier to context-free languages and Chomsky's classification of languages suggest that not every language is regular. We will prove this by giving an example of a nonregular language.

To construct the example, note that because a finite-state automaton can assume only a finite number of states and because there are infinitely many input sequences, by the pigeonhole principle there must be at least one state to which the automaton returns over and over again. This is the essential feature of an automaton that makes it possible to find a nonregular language.

Example 12.2.8 Showing That a Language Is Not Regular

Let the language L consist of all strings of the form $a^k b^k$, where k is a positive integer. Symbolically, L is the language over the alphabet $\Sigma = \{a, b\}$ defined by

$$L = \{w \in \Sigma^* \mid w = a^k b^k, \text{ where } k \text{ is a positive integer}\}.$$

Use the pigeonhole principle to show that L is not regular. In other words, show that there is no finite-state automaton that accepts L.

Solution *[Use a proof by contradiction.]* Suppose not. That is, suppose there is a finite-state automaton A that accepts L. *[A contradiction will be derived.]* Since A has only a finite number of states, these states can be denoted $s_1, s_2, s_3, \ldots, s_n$, where n is a positive integer. Consider all input strings that consist entirely of a's: $a, a^2, a^3, a^4, \ldots$. Now there are infinitely many such strings and only finitely many states. Thus, by the pigeonhole principle, there must be a state s_m and two input strings a^p and a^q with $p \neq q$ such that when either a^p or a^q is input to A, A goes to state s_m. (See Figure 12.2.6.) *[The pigeons are the strings of a's, the pigeonholes are the states, and the correspondence associates each string with the state to which A goes when the string is input.]*

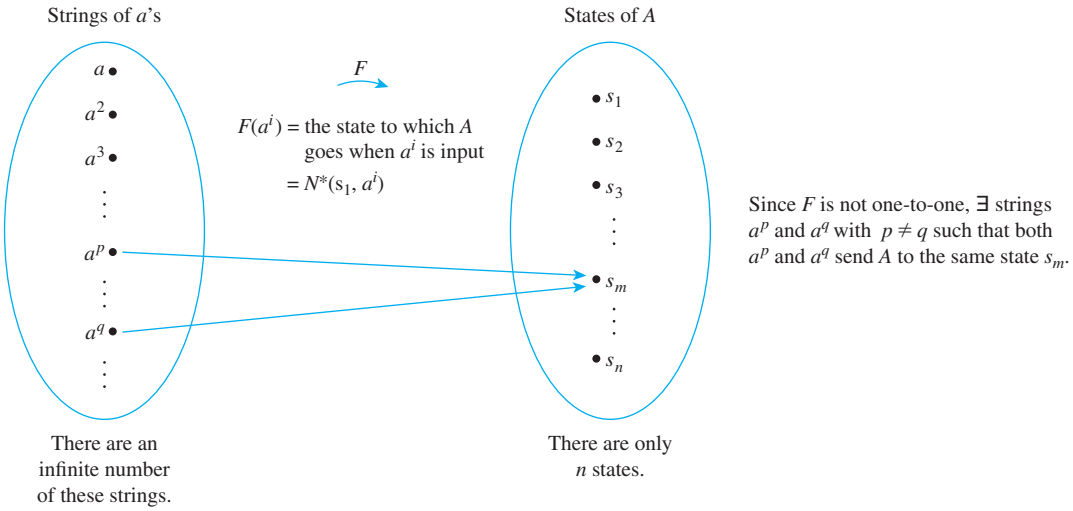


FIGURE 12.2.6

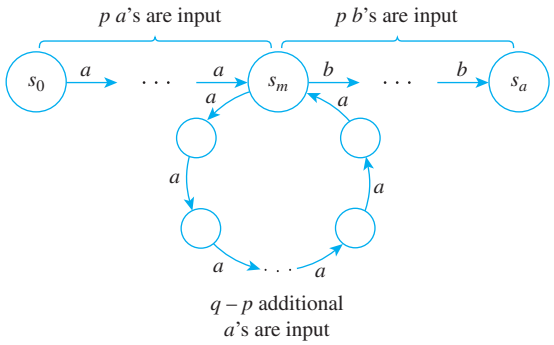
Now, by supposition, A accepts L. Hence A accepts the string

$$a^p b^p.$$

This means that after p a's have been input, at which point A is in state s_m, inputting p additional b's sends A into an accepting state, say s_a. But that implies that

$$a^q b^p$$

also sends A to the accepting state s_a, and so $a^q b^p$ is accepted by A. The reason is that after q a's have been input, A is also in state s_m, and from that point, inputting p additional b's sends A to state s_a, which is an accepting state. Pictorially, if $p < q$, then



Now, by supposition, L is the language accepted by A. Thus since $a^q b^p$ is accepted by A, $a^q b^p \in L$. But by definition of L, L consists only of strings with equal numbers of a's and b's. So since $p \neq q$, $a^q b^p \notin L$. Hence $a^q b^p \in L$ and $a^q b^p \notin L$, which is a contradiction.

It follows that the supposition is false, and so there is no finite-state automaton that accepts L. ■

TEST YOURSELF

1. The five objects that make up a finite-state automaton are _____, _____, _____, _____, and _____.
2. The next-state table for an automaton shows the values of _____.
3. In the annotated next-state table, the initial state is indicated with an _____ and the accepting states are marked by _____.
4. A string w consisting of input symbols is accepted by a finite-state automaton A if, and only if, _____.
5. The language accepted by a finite-state automaton A is _____.
6. If N is the next-state function for a finite-state automaton A, the eventual-state function N^* is defined as follows: For each state s of A and for each string w that consists of input symbols of A, $N^*(s, w) =$ _____.
7. One part of Kleene's theorem says that given any language that is accepted by a finite-state automaton, there is _____.
8. The second part of Kleene's theorem says that given any language defined by a regular expression, there is _____.
9. A regular language is _____.
10. Given the language consisting of all strings of the form $a^k b^k$, where k is a positive integer, the pigeonhole principle can be used to show that the language is _____.

EXERCISE SET 12.2

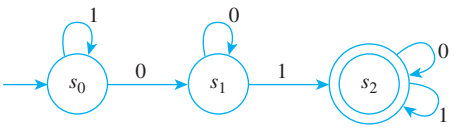
1. Find the state of the vending machine in Example 12.2.1 after each of the following sequences of coins have been input.
   a. Quarter, half-dollar, quarter
   b. Quarter, half-dollar, half-dollar
   c. Half-dollar, quarter, quarter, quarter, half-dollar

In 2–7, a finite-state automaton is given by a transition diagram. For each automaton:

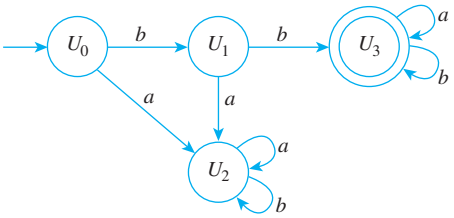
a. Find its states.

b. Find its input symbols.
c. Find its initial state.
d. Find its accepting states.
e. Write its annotated next-state table.

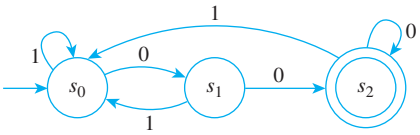
2.



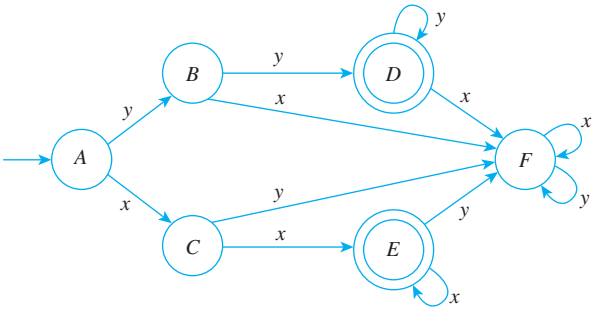
3.



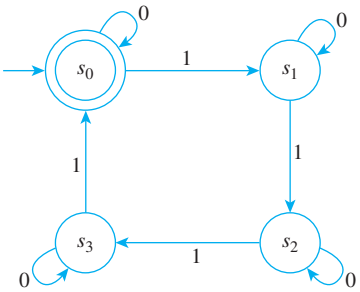
4.



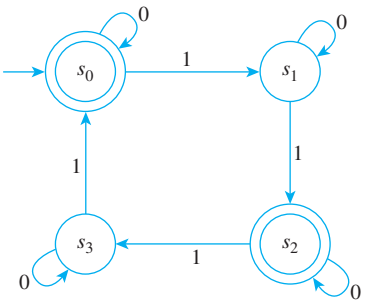
5.



6.



7.



In 8 and 9, a finite-state automaton is given by an annotated next-state table. For each automaton:
a. Find its states.
b. Find its input symbols.
c. Find its initial state.
d. Find its accepting states.
e. Draw its transition diagram.

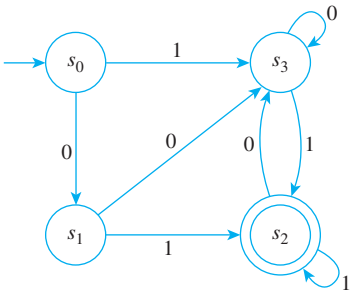
8. Next-State Table

State		Input 0	Input 1
	→	s_0	s_1	s_2
		s_1	s_1	s_2
	◎	s_2	s_1	s_2

9. Next-State Table

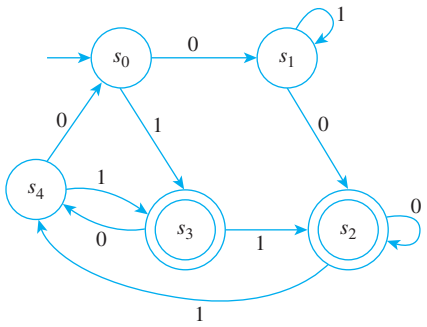
State		Input 0	Input 1
	→	s_0	s_0	s_1
	◎	s_1	s_1	s_2
		s_2	s_2	s_3
		s_3	s_3	s_0

10. A finite-state automaton A, given by the transition diagram below, has next-state function N and eventual-state function N^*.



a. Find $N(s_1, 1)$ and $N(s_0, 1)$.
b. Find $N(s_2, 0)$ and $N(s_1, 0)$.
c. Find $N^*(s_0, 10011)$ and $N^*(s_1, 01001)$.
d. Find $N^*(s_2, 11010)$ and $N^*(s_0, 01000)$.

11. A finite-state automaton A, given by the transition diagram on the next page, has next-state function N and eventual-state function N^*.



a. Find $N(s_3, 0)$ and $N(s_2, 1)$.
b. Find $N(s_0, 0)$ and $N(s_4, 1)$.
c. Find $N^*(s_0, 010011)$ and $N^*(s_3, 01101)$.
d. Find $N^*(s_0, 1111)$ and $N^*(s_2, 00111)$.

12. Consider again the finite-state automaton of exercise 2.
a. To what state does the automaton go when the symbols of the following strings are input to it in sequence, starting from the initial state?
(i) 1110001 (ii) 0001000 (iii) 11110000
b. Which of the strings in part (a) send the automaton to an accepting state?
c. What is the language accepted by the automaton?
d. Find a regular expression that defines the language.

13. Consider again the finite-state automaton of exercise 3.
a. To what state does the automaton go when the symbols of the following strings are input to it in sequence, starting from the initial state?
(i) *bb* (ii) *aabbbaba* (iii) *babbbbbabaa* (iv) *bbaaaabaa*
b. Which of the strings in part (a) send the automaton to an accepting state?
c. What is the language accepted by the automaton?
d. Find a regular expression that defines the language.

In each of 14–19, (a) find the language accepted by the automaton in the referenced exercise, and (b) find a regular expression that defines the same language.

14. Exercise 4 **15.** Exercise 5 **16.** Exercise 6
17. Exercise 7 **18.** Exercise 8 **19.** Exercise 9

In each of 20–28, (a) design an automaton with the given input alphabet that accepts the given set of strings, and (b) find a regular expression that defines the language accepted by the automaton.

20. Input alphabet = {0, 1}; Accepts the set of all strings for which the final three input symbols are 1.

21. Input alphabet = {0, 1}; Accepts the set of all strings that start with 01.

***H* 22.** Input alphabet = {*a*, *b*}; Accepts the set of all strings of length at least 2 for which the final two input symbols are the same.

23. Input alphabet = {0, 1}; Accepts the set of all strings that start with 01 or 10.

24. Input alphabet = {0, 1}; Accepts the set of all strings that start with 101.

25. Input alphabet = {0, 1}; Accepts the set of all strings that end in 10.

26. Input alphabet = {*a*, *b*}; Accepts the set of all strings that contain exactly two *b*'s.

27. Input alphabet = {0, 1}; Accepts the set of all strings that start with 0 and contain exactly one 1.

28. Input alphabet = {0, 1}; Accepts the set of all strings that contain the pattern 010.

In 29–47, design a finite-state automaton to accept the language defined by the regular expression in the referenced exercise from Section 12.1.

29. Exercise 16 **30.** Exercise 17 **31.** Exercise 18
32. Exercise 19 **33.** Exercise 20 **34.** Exercise 21
35. Exercise 24 **36.** Exercise 25 **37.** Exercise 26
38. Exercise 27 **39.** Exercise 31 **40.** Exercise 32
41. Exercise 33 **42.** Exercise 34 **43.** Exercise 35
44. Exercise 36 **45.** Exercise 37 **46.** Exercise 38
47. Exercise 39

48. A simplified telephone switching system allows the following strings as legal telephone numbers:
a. A string of seven digits in which neither of the first two digits is a 0 or 1 (*a local call string*).
b. A 1 followed by a three-digit *area code string* (any digit except 0 or 1 followed by a 0 or 1 followed by any digit) followed by a seven-digit local call string.
c. A 0 alone or followed by a three-digit area code string plus a seven-digit local call string.

Design a finite-state automaton to recognize all the legal telephone numbers in (a), (b), and (c). Include an "error state" for invalid telephone numbers.

49. Write a computer algorithm that simulates the action of the finite-state automaton of exercise 2 by mimicking the action of the transition diagram.

50. Write a computer algorithm that simulates the action of the finite-state automaton of exercise 8 by repeated application of the next-state function.

H 51. Let L be the language consisting of all strings of the form

$a^m b^n$, where m and n are positive integers and $m \geq n$.

Show that there is no finite-state automaton that accepts L.

52. Let L be the language consisting of all strings of the form

$a^m b^n$, where m and n are positive integers and $m \leq n$.

Show that there is no finite-state automaton that accepts L.

H 53. Let L be the language consisting of all strings of the form

a^n, where $n = m^2$, for some positive integer m.

Show that there is no finite-state automaton that accepts L.

54. a. Let A be a finite-state automaton with input alphabet Σ, and suppose $L(A)$ is the language accepted by A. The complement of $L(A)$ is the set of all strings over Σ that are not in $L(A)$. Show that the complement of a regular language is regular by proving the following: If $L(A)$ is the language accepted by a finite-state automaton A, then there is a finite-state automaton A' that accepts the complement of $L(A)$.

b. Show that the intersection of any two regular languages is regular as follows: First prove that if $L(A_1)$ and $L(A_2)$ are languages accepted by automata A_1 and A_2, respectively, then there is an automaton A that accepts $(L(A_1))^c \cup (L(A_2))^c$. Then use one of De Morgan's laws for sets, the double complement law for sets, and the result of part (a) to prove that there is an automaton that accepts $L(A_1) \cap L(A_2)$.

ANSWERS FOR TEST YOURSELF

1. a finite set of input symbols; a finite set of states; a designated initial state; a designated set of accepting states; a next-state function that associates a "next-state" with each state and input symbol of the automaton **2.** the next-state function for each state and input symbol of the automaton **3.** arrow; double circles **4.** when the symbols in the string are input to the automaton in sequence from left to right, starting from the initial state, the automaton ends up in an accepting state **5.** the set of strings that are accepted by A **6.** the state to which A goes if it is in state s and the characters of w are input to it in sequence **7.** a regular expression that defines the same language **8.** a finite-state automaton that accepts the same language **9.** a language defined by a regular expression (*Or*: a language accepted by a finite-state automaton) **10.** not regular

12.3 Simplifying Finite-State Automata

Our life is frittered away by detail. . . . Simplify, simplify.
—Henry David Thoreau, *Walden*, 1854

Any string input to a finite-state automaton either sends the automaton to an accepting state or not, and the set of all strings accepted by an automaton is the language accepted by the automaton. It often happens that when an automaton is created to do a certain job (as in compiler construction, for example), the automaton that emerges "naturally" from the development process is unnecessarily complicated; that is, there may be an automaton with fewer states that accepts exactly the same language. It is desirable to find such

an automaton because the memory space required to store an automaton with n states is approximately proportional to n^2. Thus approximately 10,000 memory locations are required to store an automaton with 100 states, whereas only about 100 memory locations are needed to store an automaton with 10 states. In addition, the fewer states an automaton has, the easier it is to write a computer algorithm based on it; and to see that two automata both accept the same language, it is easiest to simplify each to a minimal number of states and compare the simplified automata. In this section we show how to take a given automaton and simplify it in the sense of finding an automaton with fewer states that accepts the same language.

Example 12.3.1 **An Overview**

Consider the finite-state automata A and A' in Figure 12.3.1. A moment's thought should convince you that A' accepts all those strings, and only those strings, that contain an even number of 1's. But A, although it appears more complicated, accepts exactly those strings also. Thus the two automata are "equivalent" in the sense that they accept the same language, even though A' has fewer states than A.

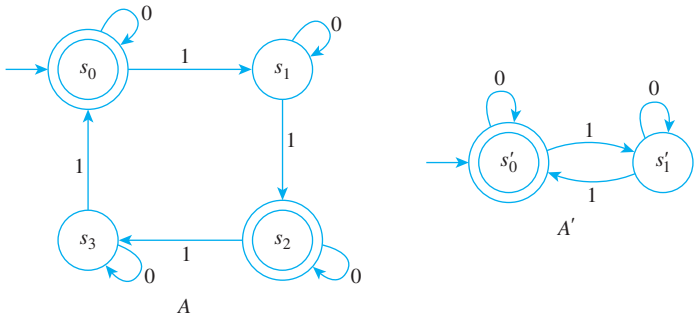


FIGURE 12.3.1 Two Equivalent Automata

Roughly speaking, the reason for the equivalence of these automata is that some of the states of A can be combined without affecting the acceptance or nonacceptance of any input string. It turns out that s_2 can be combined with state s_0 and that s_3 can be combined with state s_1. (How to figure out which states can be combined is explained later in this section.) The automaton with the two combined states $\{s_0, s_2\}$ and $\{s_1, s_3\}$ is called the *quotient automaton* of A and is denoted $\overline{A}$. Its transition diagram is obtained by combining the circles for s_0 and s_2 and for s_1 and s_3 and by replacing any arrow from a state s to a state t by an arrow from the combined state containing s to the combined state containing t. For instance, since there is an arrow labeled 1 from s_1 to s_2 in A, there is an arrow labeled 1 from $\{s_1, s_3\}$ to $\{s_0, s_2\}$ in $\overline{A}$. The complete transition diagram for $\overline{A}$ is shown in Figure 12.3.2. As you can see, except for labeling the names of the states, it is identical to the diagram for A'.

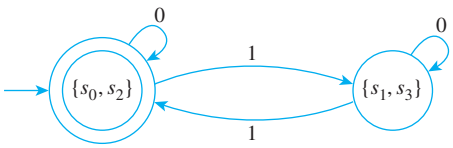


FIGURE 12.3.2 Transition Diagram for $\overline{A}$ ■

In general, simplification of a finite-state automaton involves identifying "equivalent states" that can be combined without affecting the action of the automaton on input strings. Mathematically speaking, this means defining an equivalence relation on the set of states

of the automaton and forming a new automaton whose states are the equivalence classes of the relation. The rest of this section is devoted to developing an algorithm to carry out this process in a practical way.

∗-Equivalence of States

Two states of a finite-state automaton are said to be ∗-*equivalent* (this is read "star equivalent") if, and only if, any string accepted by the automaton when it starts from one of the states is accepted by the automaton when it starts from the other state. Recall that the value of the eventual-state function, N^*, for a state s and input string w is the state to which the automaton goes if the characters of w are input in sequence when the automaton is in state s.

Definition

Let A be a finite-state automaton with next-state function N and eventual-state function N^*. Define a binary relation on the set of states of A as follows: Given any states s and t of A, we say that ***s* and *t* are ∗-equivalent** and write $s \; R_* \; t$ if, and only if, for each input string w,

either both $N^*(s, w)$ and $N^*(t, w)$ are accepting states or both are nonaccepting states.

In other words, states s and t are **∗-equivalent** if, and only if, for each input string w,

$$N^*(s, w) \text{ is an accepting state} \iff N^*(t, w) \text{ is an accepting state.}$$

Or, more simply, for each input string w,

$$\begin{bmatrix} A \text{ goes to an accepting state if} \\ w \text{ is input when } A \text{ is in state } s \end{bmatrix} \iff \begin{bmatrix} A \text{ goes to an accepting state if} \\ w \text{ is input when } A \text{ is in state } t \end{bmatrix}.$$

It follows immediately, by substitution into the definition, that

R_* is an equivalence relation on S, the set of states of A. 12.3.1

You are asked to prove this formally in the exercises at the end of this section.

k-Equivalence of States

From a procedural point of view, it is difficult to determine the ∗-equivalence of two states using the definition directly. According to the definition, you must know the action of the automaton starting in states s and t on *all* input strings in order to tell whether s and t are equivalent. But since most languages have infinitely many input strings, you cannot check individually the effect of every string that is input to an automaton. As a practical matter, you can tell whether or not two states s and t are ∗-equivalent by using an iterative procedure based on a simpler kind of equivalence of states called *k-equivalence.* Two states are *k-equivalent* if, and only if, any string *of length less than or equal to k* that is accepted by the automaton when it starts from one of the states is accepted by the automaton when it starts from the other state.

Definition

Let A be a finite-state automaton with next-state function N and eventual-state function N^*. Define a relation on the set of states of A as follows: Given any states s and t of A and an integer $k \geq 0$, we say that s is ***k*-equivalent** to t and write $s \; \boldsymbol{R_k} \; t$ if, and only if, for every input string w *of length less than or equal to* k, either $N^*(s, w)$ and $N^*(t, w)$ are both accepting states or they are both nonaccepting states.

Certain useful facts follow quickly from the definition of k-equivalence:

For each integer $k \geq 0$, k-equivalence is an equivalence relation.	12.3.2
For each integer $k \geq 0$, the k-equivalence classes partition the set of all states of the automaton into a union of mutually disjoint subsets.	12.3.3
For each integer $k \geq 1$, if two states are k-equivalent, then they are also $(k-1)$ equivalent.	12.3.4
For each integer $k \geq 1$, each k-equivalence class is a subset of a $(k-1)$-equivalence class.	12.3.5
Any two states that are k-equivalent for every integer $k \geq 0$ are $*$-equivalent.	12.3.6

Proofs of these facts are left for the exercises.

The following theorem gives a recursive description of k-equivalence of states. It says, first, that any two states are 0-equivalent if, and only if, either both are accepting states or both are nonaccepting states and, second, that any two states are k-equivalent (for $k \geq 1$) if, and only if, (1) they are $(k-1)$-equivalent and (2) for any input symbols their next-states are also $(k-1)$-equivalent.

Theorem 12.3.1

Let A be a finite-state automaton with next-state function N. Given any states s and t in A,

1. s is 0-equivalent to t $\Leftrightarrow$ [either s and t are both accepting states or they are both nonaccepting states]

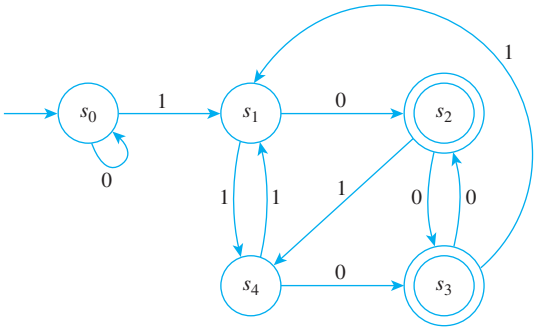
2. for every integer $k \geq 1$, s is k-equivalent to t $\Leftrightarrow$ [s and t are $(k-1)$-equivalent, and for any input symbol m, $N(s, m)$ and $N(t, m)$ are also $(k-1)$-equivalent].

The truth of Theorem 12.3.1 follows from the fact that inputting a string w of length k has the same effect as inputting the first symbol of w and then the remaining $k-1$ symbols of w. A detailed proof is somewhat technical.

Theorem 12.3.1 implies that if you know which states are $(k-1)$-equivalent (where k is a positive integer) and if you know the action of the next-state function, then you can figure out which states are k-equivalent. Specifically, if s and t are $(k-1)$-equivalent states whose next-states are $(k-1)$-equivalent for every input symbol m, then s and t are k-equivalent. Thus the k-equivalence classes are obtained by subdividing the $(k-1)$-equivalence classes according to the action of the next-state function on the members of the classes. An example should make this procedure clear.

Example 12.3.2 **Finding *k*-Equivalence Classes**

Find the 0-equivalence classes, the 1-equivalence classes, and the 2-equivalence classes for the states of the automaton shown below.



Solution

1. **0-*equivalence classes:*** By Theorem 12.3.1 two states are 0-equivalent if, and only if, both are accepting states or both are nonaccepting states. Thus there are two sets of 0-equivalent states:

   $\{s_0, s_1, s_4\}$ (the nonaccepting states) and $\{s_2, s_3\}$ (the accepting states),

   and so

   the 0-equivalence classes are $\{s_0, s_1, s_4\}$ and $\{s_2, s_3\}$.

2. **1-*equivalence classes:*** By Theorem 12.3.1, two states are 1-equivalent if, and only if, they are 0-equivalent and, after input of any input symbol, their next-states are 0-equivalent. Thus s_1 is not 1-equivalent to s_0 because when a 0 is input to the automaton in state s_1 it goes to state s_2, whereas when a 0 is input to the automaton in state s_0 it goes to state s_0, and s_2 and s_0 are not 0-equivalent. On the other hand, s_1 *is* 1-equivalent to s_4 because when a 0 is input to the automaton in state s_1 or s_4 the next-states are s_2 and s_3, which are 0-equivalent; and when a 1 is input to the automaton in state s_1 or s_4 the next-states are s_4 and s_1, which are 0-equivalent. By a similar argument, s_2 is 1-equivalent to s_3. Since 1-equivalent states must also be 0-equivalent *[by property* (12.3.4)*]*, no other pairs of states can be 1-equivalent. Hence

   the 1-equivalence classes are $\{s_0\}$, $\{s_1, s_4\}$, and $\{s_2, s_3\}$.

3. **2-*equivalence classes:*** By Theorem 12.3.1, two states are 2-equivalent if, and only if, they are 1-equivalent and, after input of any input symbol, their next-states are 1-equivalent. Now s_1 is 2-equivalent to s_4 because they are 1-equivalent; and when a 1 is input to the automaton in state s_1 or s_4 the next-states are s_4 and s_1, which are 1-equivalent; and when a 0 is input to the automaton in state s_1 or s_4 the next-states are s_2 and s_3, which are 1-equivalent. Similarly, s_2 is 2-equivalent to s_3. Since 2-equivalent states must also be 1-equivalent *[by property* (12.3.4)*]*, no other pairs of states can be 2-equivalent. Hence

   the 2-equivalence classes are $\{s_0\}$, $\{s_1, s_4\}$, and $\{s_2, s_3\}$.

   Note that the set of 2-equivalence classes equals the set of 1-equivalence classes. ■

Finding the $*$-Equivalence Classes

Example 12.3.2 illustrates the relative ease with which the sets of k-equivalence classes of states can be found. But to simplify a finite-state automaton, you need to find the set of $*$-equivalence classes of states. The next theorem says that for some integer K, the set of $*$-equivalence classes equals the set of K-equivalence classes.

Theorem 12.3.2

If A is a finite-state automaton, then for some integer, $K \geq 0$, the set of K-equivalence classes of states of A equals the set of $(K+1)$-equivalence classes of states of A, and for all such K these are both equal to the set of $*$-equivalence classes of states of A.

The detailed proof of Theorem 12.3.2 is somewhat technical, but the idea of the proof is not hard to understand. Theorem 12.3.2 follows from the fact that for each positive integer k, the k-equivalence classes are obtained by subdividing the $(k-1)$-equivalence classes according to a certain rule that is the same for each k. Since the number of states of the automaton is finite, this subdivision process cannot continue forever, and so for some integer $K \geq 0$, the set of K-equivalence classes equals the set of $(K+1)$-equivalence classes. Moreover, the set of m-equivalence classes equals the set of K-equivalence classes for every integer $m \geq K$, which implies that the set of $*$-equivalence classes equals the set of K-equivalence classes.

Example 12.3.3 **Finding $*$-Equivalence Classes of R**

Let A be the finite-state automaton defined in Example 12.3.2. Find the $*$-equivalence classes of states of A.

Solution According to Example 12.3.2, the set of 1-equivalence classes for A equals the set of 2-equivalence classes. By Theorem 12.3.2, then, the set of $*$-equivalence classes also equals the set of 1-equivalence classes. Hence

$$\text{the } *\text{-equivalence classes are } \{s_0\},\ \{s_1, s_4\}, \text{ and } \{s_2, s_3\}.$$

In the notation of Section 8.3, the equivalence classes are denoted

$$[s_0] = \{s_0\} \quad [s_1] = \{s_1, s_4\} = [s_4] \quad [s_2] = \{s_2, s_3\} = [s_3].$$ ■

The Quotient Automaton

We next define the *quotient automaton* $\overline{A}$ of an automaton A. However, in order for all parts of the definition to make sense, we must make two observations.

No $*$-equivalence class of states of A can contain both accepting and nonaccepting states. 12.3.7

The reason this is true is that the 0-equivalence classes divide the set of states of A into accepting and nonaccepting states, and the $*$-equivalence classes are subsets of 0-equivalence classes.

If two states are $*$-equivalent, then their next-states are also $*$-equivalent for each input symbol m. 12.3.8

This is true for the following reason. Suppose states s and t are $*$-equivalent. Then any input string that sends A to an accepting state when A is in state s sends A to an accepting state when A is in state t. Now suppose m is any input symbol, and consider the next-states $N(s, m)$ and $N(t, m)$. Inputting a string of length k to A when A is in state $N(s, m)$ or $N(t, m)$ produces the same effect as inputting a certain string of length $k + 1$ to A when A is in state s or t (namely, the concatenation of m with the string of length k). Hence any string that sends A to an accepting state when A is in state $N(s, m)$ also sends A to an accepting state when A is in state $N(t, m)$. It follows that $N(s, m)$ and $N(t, m)$ are $*$-equivalent. Complete proofs of properties (12.3.7) and (12.3.8) are left to the exercises.

Now we can define the quotient automaton $\overline{A}$ of A. It is the finite-state automaton whose states are the $*$-equivalence classes of states of A, whose initial state is the $*$-equivalence class containing the initial state of A, whose accepting states are of the form $[s]$ where s is an accepting state of A, whose input symbols are the same as the input symbols of A, and whose next-state function is derived from the next-state function for A in the following way: To find the next-state of $\overline{A}$ for a state s and an input symbol m, pick any state t in $[s]$ and look to see what next-state A goes to if m is input when A is in state t; the equivalence class of this state is the next-state of $\overline{A}$.

Definition

Let A be a finite-state automaton with set of states S, set of input symbols I, and next-state function N. The **quotient automaton** $\overline{A}$ is defined as follows:

1. The set of states, $\overline{S}$, of $\overline{A}$ is the set of $*$-equivalence classes of states of A.
2. The set of input symbols, $\overline{I}$, of $\overline{A}$ equals I.
3. The initial state of $\overline{A}$ is $[s_0]$, where s_0 is the initial state of A.
4. The accepting states of $\overline{A}$ are the states of the form $[s]$, where s is an accepting state of A.
5. The next-state function $\overline{N}$: $\overline{S} \times I \longrightarrow \overline{S}$ is defined as follows:

   For all states $[s]$ in $\overline{S}$ and input symbols m in I, $\quad \overline{N}([s], m) = [N(s, m)]$.

   (That is, if m is input to $\overline{A}$ when $\overline{A}$ is in state $[s]$, then $\overline{A}$ goes to the state that is the $*$-equivalence class of $N(s, m)$.)

Note that since the states of $\overline{A}$ are *sets* of states of A, $\overline{A}$ generally has fewer states than A. (A and $\overline{A}$ have the same number of states only in the case where each $*$-equivalence class of states contains just one element.) Also, by property (12.3.7), each accepting state of $\overline{A}$ consists entirely of accepting states of A. Furthermore, property (12.3.8) guarantees that the next-state function $\overline{N}$ is well defined.

By construction, a quotient automaton $\overline{A}$ accepts exactly the same strings as A. We state this formally as Theorem 12.3.3 and leave the details of a proof to a more advanced course in automata theory.

Theorem 12.3.3

If A is a finite-state automaton, then the quotient automaton $\overline{A}$ accepts exactly the same languages as A. In other words, if $L(A)$ denotes the language accepted by A and $L(\overline{A})$ denotes the language accepted by $\overline{A}$, then

$$L(A) = L(\overline{A}).$$

Constructing the Quotient Automaton

Let A be a finite-state automaton with set of states S, next-state function N, relation R_* of $*$-equivalence of states, and relation R_k of k-equivalence of states. It follows from Theorems 12.3.2 and 12.3.3 and from the definition of quotient automaton that to find the quotient automaton $\overline{A}$ of A, you can proceed as follows:

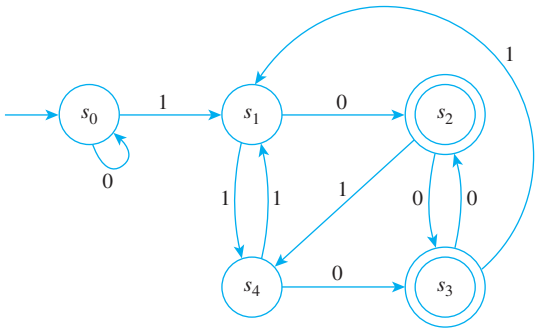
1. Find the set of 0-equivalence classes of S.
2. For each integer $k \geq 1$, subdivide the $(k-1)$-equivalence classes of S (as described earlier) to find the k-equivalence classes of S. Stop subdividing when you observe that for some integer K the set of $(K+1)$-equivalence classes equals the set of K-equivalence classes. At this point, conclude that the set of K-equivalence classes equals the set of $*$-equivalence classes.
3. Construct the quotient automaton $\overline{A}$ whose states are the $*$-equivalence classes of states of A and whose next-state function $\overline{N}$ is given by

$$\overline{N}([s], m) = [N(s, m)] \qquad \text{for each state } s \text{ of } \overline{A} \text{ and each input symbol } m.$$

[That is, to see where $\overline{A}$ goes if m is input to $\overline{A}$ when it is in state $[s]$, look to see where A goes if m is input to A when it is in state s. The $*$-equivalence class of that state is the answer.]

Example 12.3.4 **Constructing a Quotient Automaton**

Consider the automaton A of Examples 12.3.2 and 12.3.3. This automaton is shown again below for reference. Find the quotient automaton of A.



Solution According to Example 12.3.3, the $*$-equivalence classes of the states of A are

$$\{s_0\}, \quad \{s_1, s_4\}, \quad \text{and} \quad \{s_2, s_3\}.$$

Hence the states of the quotient automaton $\overline{A}$ are

$$[s_0] = \{s_0\}, \quad [s_1] = \{s_1, s_4\} = [s_4], \quad [s_2] = \{s_2, s_3\} = [s_3].$$

The accepting states of A are s_2 and s_3, so the accepting state of $\overline{A}$ is $[s_2] = [s_3]$. The next-state function $\overline{N}$ of $\overline{A}$ is defined as follows: for all states $[s]$ and input symbols m of $\overline{A}$,

$$\overline{N}([s], m) = [N(s, m)] = \text{the } *\text{-equivalence class of } N(s, m).$$

Thus

$$\overline{N}([s_0], 0) = [N(s_0, 0)] = \text{the } *\text{-equivalence class of } N(s_0, 0).$$

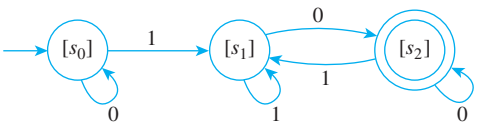
Now $N(s_0, 0) = s_0$, and so

$$\overline{N}([s_0], 0) = \text{the } *\text{-equivalence class of } s_0 = [s_0].$$

Similarly,

$$\overline{N}([s_0], 1) = [N(s_0, 1)] = [s_1]$$
$$\overline{N}([s_1], 0) = [N(s_1, 0)] = [s_2]$$
$$\overline{N}([s_1], 1) = [N(s_1, 1)] = [s_4] = [s_1]$$
$$\overline{N}([s_2], 0) = [N(s_2, 0)] = [s_3] = [s_2]$$
$$\overline{N}([s_2], 1) = [N(s_2, 1)] = [s_4] = [s_1].$$

The transition diagram for $\overline{A}$ is, therefore, as shown below.



By Theorem 12.3.3, this automaton accepts the same language as the original automaton. ■

Equivalent Automata

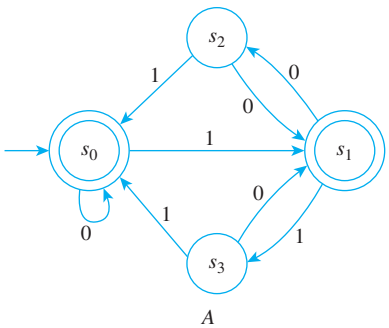
When a finite-state automaton is implemented by a circuit, output indicators may be attached to its states to indicate whether they are accepting or nonaccepting. For example, accepting states might produce an output of 1 and nonaccepting states an output of 0. Then a finite-state automaton can be thought of as an input/output device whose input consists of strings and whose output consists of 0's and 1's. Recall that a circuit can be thought of as a black box that transforms combinations of input signals into output signals. Two circuits that produce identical output signals for each combination of input signals are called *equivalent*. Similarly, a finite-state automaton can be regarded as a black box that processes input strings and produces output signals (indicating whether or not the strings are accepted). Two finite-state automata are called *equivalent* if they produce identical output signals for each input string. This implies that two finite-state automata are equivalent if, and only if, they accept the same language.

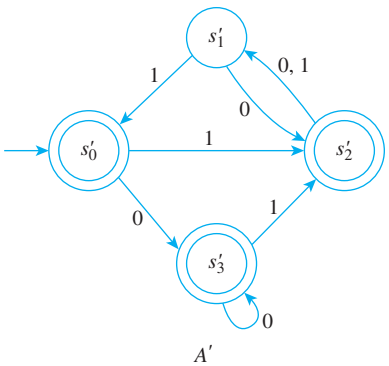
Definition

Let A and A' be finite-state automata with the same set of input symbols I. Let $L(A)$ denote the language accepted by A and $L(A')$ the language accepted by A'. Then A is said to be **equivalent** to A' if, and only if, $L(A) = L(A')$.

Example 12.3.5 **Showing That Two Automata Are Equivalent**

Show that the automata A and A' that follow are equivalent.





The label 0, 1 on an arrow of a transition diagram means that for either input 0 or 1, the next-state of the automaton is the state to which the arrow points.

Solution

For the automaton A: The 0-equivalence classes are

$$\{s_0, s_1\} \quad \text{and} \quad \{s_2, s_3\}$$

since s_0 and s_1 are accepting states and s_2 and s_3 are nonaccepting states.

The 1-equivalence classes are

$$\{s_0\}, \quad \{s_1\}, \quad \text{and} \quad \{s_2, s_3\}$$

since s_0 and s_1 are not 1-equivalent (because $N(s_0, 1) = s_1$, and $N(s_1, 1) = s_3$, and s_1 is not 0-equivalent to s_3) but s_2 and s_3 are 1-equivalent.

The 2-equivalence classes are

$$\{s_0\}, \quad \{s_1\}, \quad \text{and} \quad \{s_2, s_3\}$$

since s_2 and s_3 are 1-equivalent.

This discussion shows that the set of 1-equivalence classes equals the set of 2-equivalence classes, so by Theorem 12.3.2 this is equal to the set of $*$-equivalence classes. Hence the $*$-equivalence classes are

$$\{s_0\}, \quad \{s_1\}, \quad \text{and} \quad \{s_2, s_3\}.$$

For the automaton A′: By reasoning similar to that done previously, the 0-equivalence classes are

$$\{s'_0, s'_2, s'_3\}, \quad \text{and} \quad \{s'_1\}.$$

The 1-equivalence classes are

$$\{s'_0, s'_3\}, \quad \{s'_2\}, \quad \text{and} \quad \{s'_1\}.$$

The 2-equivalence classes are the same as the 1-equivalence classes, which are therefore equal to the $*$-equivalence classes. Thus the $*$-equivalence classes are

$$\{s'_0, s'_3\}, \quad \{s'_2\}, \quad \text{and} \quad \{s'_1\}.$$

To calculate the next-state functions for $\overline{A}$ and $\overline{A'}$, you repeatedly use the fact that in the quotient automaton, the next-state of $[s]$ and m is the class of the next-state of s and m. For instance,

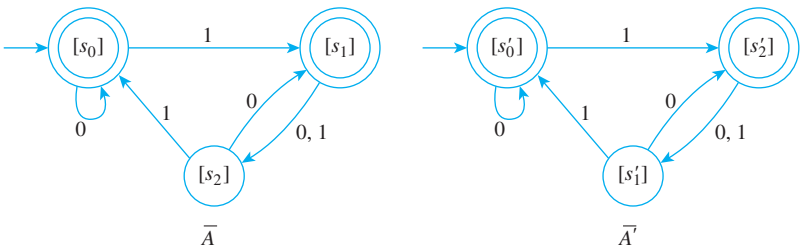
$$\overline{N}([s_1], 1) = [N(s_1, 1)] = [s_3] = [s_2]$$

and

$$\overline{N'}([s'_0], 0) = [N'(s'_0, 0)] = [s'_3] = [s'_0],$$

where N is the next-state function for A and N' is the next-state function for A'.

The complete transition diagrams for the quotient automata $\overline{A}$ and $\overline{A'}$ are shown below.



$\overline{A}$ $\overline{A'}$

As you can see, except for the labeling of the names of the states, $\overline{A}$ and $\overline{A'}$ are identical and hence accept the same language. Now by Theorem 12.3.3, each original automaton accepts the same language as its quotient automaton. Thus A and A' accept the same language, and so they are equivalent. ■

In mathematics an object such as a finite-state automaton is called a *structure*. In general, when two mathematical structures are the same in all respects except for the labeling given to their elements, they are called **isomorphic**, which comes from the Greek words

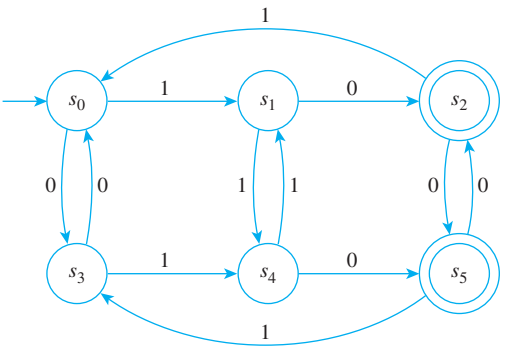
isos, meaning "same" or "equal," and *morphe*, meaning "from." It can be shown that two automata are equivalent if, and only if, their quotient automata are isomorphic, provided that "inaccessible states" have first been removed. (Inaccessible states are those that cannot be reached by inputting any string of symbols to the automaton when it is in its initial state.)

TEST YOURSELF

1. Given a finite-state automaton A with eventual-state function N^* and given any states s and t in A, we say that s and t are $*$-equivalent if, and only if, _____.
2. Given a finite-state automaton A with eventual-state function N^* and given any states s and t in A, we say that s and t are k-equivalent if, and only if, _____.
3. Given states s and t in a finite-state automaton A, s is 0-equivalent to t if, and only if, either both s and t are _____ or both are _____. Moreover, for every integer $k \geq 1$, s is k-equivalent to t if, and only if, (1) s and t are $(k-1)$-equivalent and (2) _____.
4. If A is a finite-state automaton, then for some integer $K \geq 0$, the set of K-equivalence classes of states of A equals the set of _____-equivalence classes of A, and for all such K these are both equal to the set of _____.
5. Given a finite-state automaton A, the set of states of the quotient automaton $\overline{A}$ is _____.

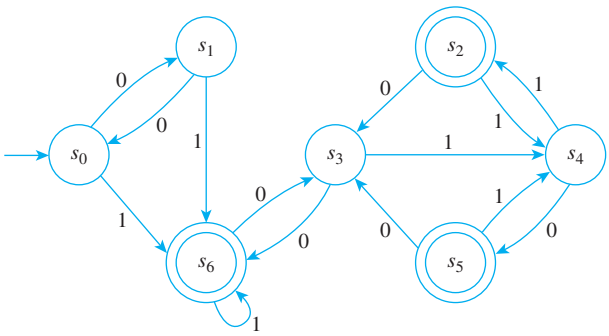
EXERCISE SET 12.3

1. Consider the finite-state automaton A given by the following transition diagram:



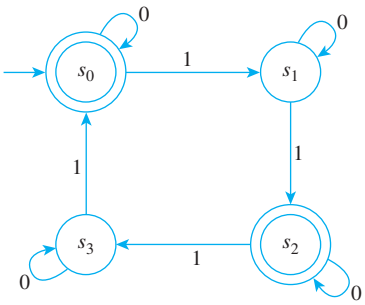
   a. Find the 0-, 1-, and 2-equivalence classes of states of A.
   b. Draw the transition diagram for $\overline{A}$, the quotient automaton of A.

2. Consider the finite-state automaton A given by the following transition diagram:



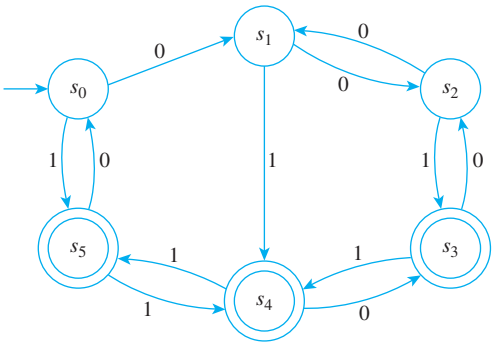
   a. Find the 0-, 1-, and 2-equivalence classes of states of A.
   b. Draw the transition diagram for $\overline{A}$, the quotient automaton of A.

3. Consider the finite-state automaton A discussed in Example 12.3.1:



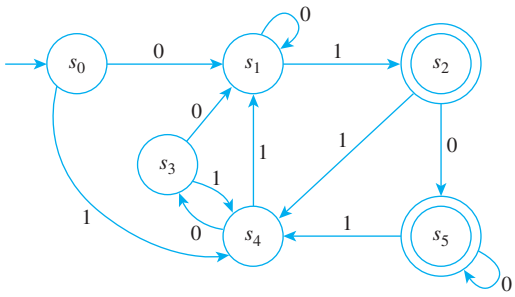
   a. Find the 0- and 1-equivalence classes of states of A.
   b. Draw the transition diagram of $\overline{A}$, the quotient automaton of A.

4. Consider the finite-state automaton given by the following transition diagram:



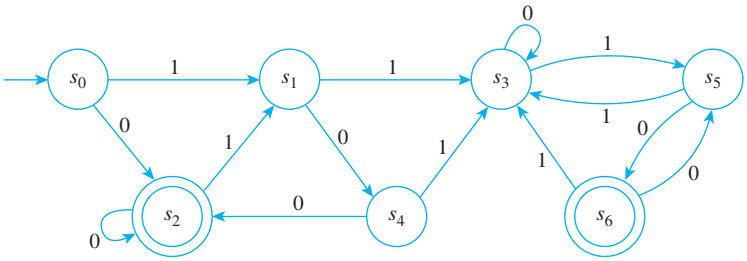
a. Find the 0-, 1-, 2-, and 3-equivalence classes of states of A.
b. Draw the transition diagram for $\overline{A}$, the quotient automaton of A.

5. Consider the finite-state automaton given by the following transition diagram:



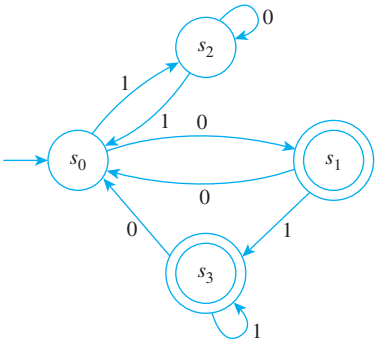
a. Find the 0-, 1-, 2-, and 3-equivalence classes of states of A.
b. Draw the transition diagram for $\overline{A}$, the quotient automaton of A.

6. Consider the finite-state automaton given by the following transition diagram:

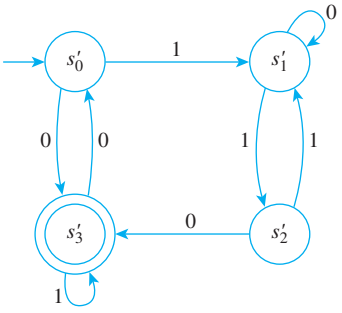


H a. Find the 0-, 1-, 2-, and 3-equivalence classes of states of A.
b. Draw the transition diagram for $\overline{A}$, the quotient automaton of A.

7. Are the automata A and A' shown below equivalent?

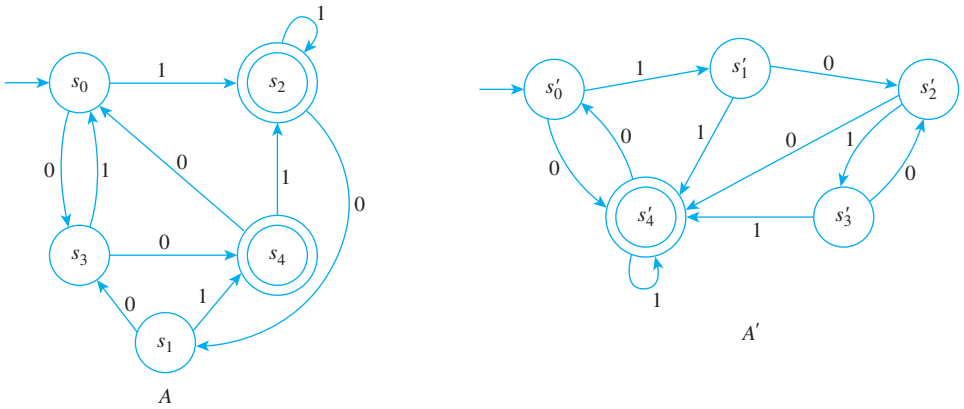


A

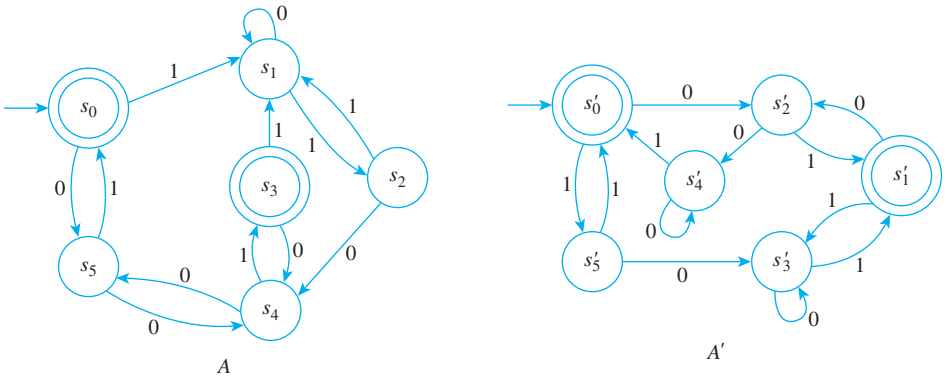


A'

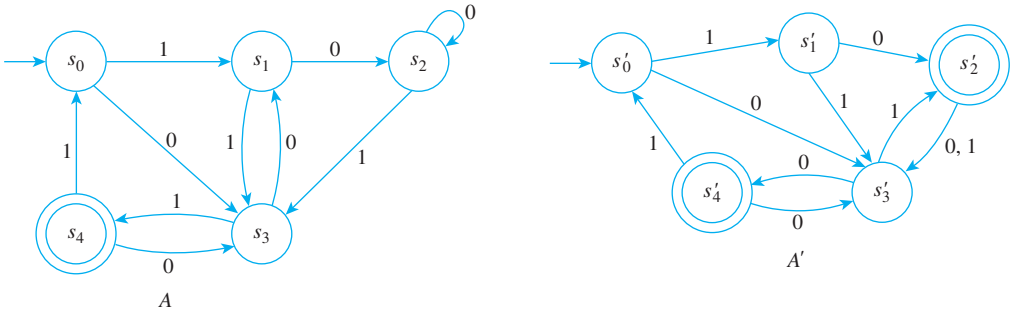
8. Are the automata A and A' shown below equivalent?



9. Are the automata A and A' shown below equivalent?



10. Are the automata A and A' shown below equivalent?



***H* 11.** Prove property (12.3.1).

12. How should the proof of property (12.3.1) be modified to prove property (12.3.2)?

13. Prove property (12.3.3).

14. Prove property (12.3.4).

***H* 15.** Prove property (12.3.5).

16. Prove property (12.3.6).

***H* 17.** Prove that if two states of a finite-state automaton are k-equivalent for some integer k, then those states are m-equivalent for every nonnegative integer $m < k$.

18. Write a complete proof of property (12.3.7).

***H* 19.** Write a complete proof of property (12.3.8).

ANSWERS FOR TEST YOURSELF

1. for all input strings w, either $N^*(s, w)$ and $N^*(t, w)$ are both accepting states or both are nonaccepting states **2.** for all input strings w of length less than or equal to k, either $N^*(s, w)$ and $N^*(t, w)$ are both accepting states or both are nonaccepting states **3.** accepting states; nonaccepting states; for any input symbol m, $N(s, m)$ and $N(t, m)$ are also $(k - 1)$-equivalent **4.** $(K + 1)$; $*$-equivalence classes of states of A **5.** the set of $*$-equivalence classes of states of A

APPENDIX A

PROPERTIES OF THE REAL NUMBERS*

In this text we take the real numbers and their basic properties as our starting point. We give a core set of properties, called axioms, which the real numbers are assumed to satisfy, and we state some useful properties that can be deduced from these axioms.

We assume that there are two binary operations defined on the set of real numbers, called **addition** and **multiplication**, such that if a and b are any two real numbers, the **sum** of a and b, denoted $\boldsymbol{a+b}$, and the **product** of a and b, denoted $\boldsymbol{a \cdot b}$ or $\boldsymbol{ab}$, are also real numbers. These operations satisfy properties F1–F6, which are called the **field axioms**.

F1. *Commutative Laws* For all real numbers a and b,

$$a+b=b+a \quad \text{and} \quad ab=ba.$$

F2. *Associative Laws* For all real numbers a, b, and c,

$$(a+b)+c=a+(b+c) \quad \text{and} \quad (ab)c=a(bc).$$

F3. *Distributive Laws* For all real numbers a, b, and c,

$$a(b+c)=ab+ac \quad \text{and} \quad (b+c)a=ba+ca.$$

F4. *Existence of Identity Elements* There exist two distinct real numbers, denoted 0 and 1, such that for every real number a,

$$0+a=a+0=a \quad \text{and} \quad 1 \cdot a=a \cdot 1=a.$$

F5. *Existence of Additive Inverses* For every real number a, there is a real number, denoted $-a$ and called the **additive inverse** of a, such that

$$a+(-a)=(-a)+a=0.$$

F6. *Existence of Reciprocals* For every real number $a \neq 0$, there is a real number, denoted $1/a$ or a^{-1}, called the **reciprocal** of a, such that

$$a \cdot \left(\frac{1}{a}\right)=\left(\frac{1}{a}\right) \cdot a=1.$$

All the usual algebraic properties of the real numbers that do not involve order can be derived from the field axioms. The most important are collected as theorems T1–T16 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

T1. *Cancellation Law for Addition* If $a+b=a+c$, then $b=c$. (In particular, this shows that the number 0 of Axiom F4 is unique.)

T2. *Possibility of Subtraction* Given a and b, there is exactly one x such that $a+x=b$. This x is denoted by $b-a$. In particular, $0-a$ is the additive inverse of a, $-a$.

*Adapted from Tom M. Apostol, *Calculus*, *Volume I* (New York: Blaisdell, 1961), pp. 13–19.

T3. $b - a = b + (-a)$.

T4. $-(-a) = a$.

T5. $a(b - c) = ab - ac$.

T6. $0 \cdot a = a \cdot 0 = 0$.

T7. *Cancellation Law for Multiplication* If $ab = ac$ and $a \neq 0$, then $b = c$. (In particular, this shows that the number 1 of Axiom F4 is unique.)

T8. *Possibility of Division* Given a and b with $a \neq 0$, there is exactly one x such that $ax = b$. This x is denoted by b/a and is called the **quotient** of b and a. In particular, $1/a$ is the reciprocal of a.

T9. If $a \neq 0$, then $b/a = b \cdot a^{-1}$.

T10. If $a \neq 0$, then $(a^{-1})^{-1} = a$.

T11. *Zero Product Property* If $ab = 0$, then $a = 0$ or $b = 0$.

T12. *Rule for Multiplication with Negative Signs*

$$(-a)b = a(-b) = -(ab), \qquad (-a)(-b) = ab,$$

and

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}.$$

T13. *Equivalent Fractions Property*

$$\frac{a}{b} = \frac{ac}{bc}, \quad \text{if } b \neq 0 \text{ and } c \neq 0.$$

T14. *Rule for Addition of Fractions*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T15. *Rule for Multiplication of Fractions*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T16. *Rule for Division of Fractions*

$$\frac{\dfrac{a}{b}}{\dfrac{c}{d}} = \frac{ad}{bc}, \quad \text{if } b \neq 0,\ c \neq 0, \text{ and } d \neq 0.$$

The real numbers also satisfy the following axioms, called the **order axioms**. It is assumed that among all real numbers there are certain ones, called the **positive real numbers**, that satisfy properties Ord1–Ord3.

Ordl. For any real numbers a and b, if a and b are positive, so are $a + b$ and ab.

Ord2. For every real number $a \neq 0$, either a is positive or $-a$ is positive but not both.

Ord3. The number 0 is not positive.

The symbols $<$, $>$, $\leq$, and $\geq$, and negative numbers are defined in terms of positive numbers.

Definition

Given real numbers a and b,

$a < b$ means $b + (-a)$ is positive. $b > a$ means $a < b$.
$a \leq b$ means $a < b$ or $a = b$. $b \geq a$ means $a \leq b$.
If $a < 0$, we say that a is **negative**. If $a \geq 0$, we say that a is **nonnegative**.

From the order axioms Ord1–Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems T17–T27 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

T17. *Trichotomy Law* For arbitrary real numbers a and b, exactly one of the three relations $a < b$, $b < a$, or $a = b$ holds.

T18. *Transitive Law* If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a + c < b + c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

One final axiom distinguishes the set of real numbers from the set of rational numbers. It is called the **least upper bound axiom**.

LUB. Any nonempty set S of real numbers that is bounded above has a least upper bound. That is, if B is the set of all real numbers x such that $x \geq s$ for every s in S and if B has at least one element, then B has a smallest element. This element is called the **least upper bound** of S.

The least upper bound axiom holds for the set of real numbers but not for the set of rational numbers. For example, the set of all rational numbers that are less than $\sqrt{2}$ has upper bounds but not a least upper bound within the set of rational numbers.

APPENDIX B SOLUTIONS AND HINTS TO SELECTED EXERCISES

SECTION 1.1

1. **a.** $x^2 = -1$ (*Or*: the square of x is -1)
b. a real number x

3. **a.** between a and b
b. distinct real numbers a and b; there is a real number c

5. **a.** r is positive
b. positive; the reciprocal of r is positive (*Or*: positive; $1/r$ is positive)
c. is positive; $1/r$ is positive (*Or*: is positive; the reciprocal of r is positive)

7. **a.** There are real numbers whose sum is less than their difference.

True. For example, $1 + (-1) = 0$, $1 - (-1) = 1 + 1 = 2$, and $0 < 2$.

c. The square of each positive integer is greater than or equal to the integer.

True. If n is any positive integer, then $n \geq 1$. Multiplying both sides by the positive number n does not change the direction of the inequality (see Appendix A, T20), and so $n^2 \geq n$.

8. **a.** have four sides
b. has four sides
c. has four sides
d. is a square; has four sides
e. J has four sides

10. **a.** have reciprocals
b. a reciprocal
c. s is a reciprocal for r

12. **a.** real number; product with every number leaves the number unchanged
b. with every number leaves the number unchanged
c. $rs = s$

SECTION 1.2

1. $A = C$ and $B = D$

2. **a.** The set of all positive real numbers x such that 0 is less than x and x is less than 1
c. The set of all integers n such that n is a factor of 6

3. **a.** No, $\{4\}$ is a set with one element, namely 4, whereas 4 is just a symbol that represents the number 4
b. Three: the elements of the set are 3, 4, and 5.
c. Three: the elements are the symbol 1, the set $\{1\}$, and the set $\{1, \{1\}\}$

5. *Hint:* $\mathbf{R}$ is the set of all real numbers, $\mathbf{Z}$ is the set of all integers, and $\mathbf{Z}^+$ is the set of all positive integers.

6. *Hint:* T_0 and T_1 do not have the same number of elements as T_2 and T_{-3}.

7. **a.** $\{1, -1\}$
c. the set has no elements
d. $\mathbf{Z}$ (every integer is in the set)

8. **a.** No, $B \not\subseteq A$ because $j \in B$ and $j \notin A$
d. Yes, C is a proper subset of A. Both elements of C are in A, but A contains elements (namely c and f) that are not in C.

9. **a.** Yes
b. No, the number 1 is not a set and so it cannot be a subset.
f. No, the only element in $\{2\}$ is the number 2 and the number 2 is not one of the three elements in $\{1, \{2\}, \{3\}\}$.
i. Yes, the only element in $\{1\}$ is the number 1, which is an element in $\{1, \{2\}\}$.

10. **a.** No. Observe that $(-2)^2 = (-2)(-2) = 4$, whereas $-2^2 = -(2^2) = -4$. So $((-2)^2, -2^2) = (4, -4)$, whereas $(-2^2, (-2)^2) = (-4, 4)$. And $(4, -4) \neq (-4, 4)$ because $-4 \neq 4$.
c. Yes. Note that $8 - 9 = -1$ and $\sqrt[3]{-1} = -1$, and so $(8 - 9, \sqrt[3]{-1}) = (-1, -1)$.

11. **a.** $\{(w, a), (w, b), (x, a), (x, b), (y, a), (y, b), (z, a), (z, b)\}$
$A \times B$ has $4 \cdot 2 = 8$ elements.
b. $\{(a, w), (b, w), (a, x), (b, x), (a, y), (b, y), (a, z), (b, z)\}$
$B \times A$ has $4 \cdot 2 = 8$ elements.
c. $\{(w, w), (w, x), (w, y), (w, z), (x, w), (x, x), (x, y), (x, z), (y, w), (y, x), (y, y), (y, z), (z, w), (z, x), (z, y), (z, z)\}$
$A \times A$ has $4 \cdot 4 = 16$ elements.
d. $\{(a, a), (a, b), (b, a), (b, b)\}$ $B \times B$ has $2 \cdot 2 = 4$ elements.

13. a. $A \times (B \times C) = \{(1, (u, m)), (1, (u, n)), (2, (u, m)), (2, (u, n)), (3, (u, m)), (3, (u, n))\}$

b. $(A \times B) \times C = \{((1, u), m), ((1, u), n), ((2, u), m), ((2, u), n), ((3, u), m), ((3, u), n)\}$

c. $A \times B \times C = \{(1, u, m), (1, u, n), (2, u, m), (2, u, n), (3, u, m), (3, u, n)\}$

15. 0000, 0001, 0010, 0100, 1000

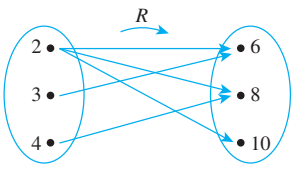
SECTION 1.3

1. a. No. Yes. No. Yes.

b. $R = \{(2, 6), (2, 8), (2, 10), (3, 6), (4, 8)\}$

c. Domain of $R = A = \{2, 3, 4\}$, co-domain of $R = B = \{6, 8, 10\}$

d.



3. a. $3\ T\ 0$ because $\frac{3-0}{3} = \frac{3}{3} = 1$, which is an integer.

$1 \not T (-1)$ because $\frac{1-(-1)}{3} = \frac{2}{3}$, which is not an integer.

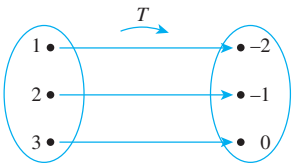
$(2, -1) \in T$ because $\frac{2-(-1)}{3} = \frac{3}{3} = 1$, which is an integer.

$(3, -2) \notin T$ because $\frac{3-(-2)}{3} = \frac{5}{3}$, which is not an integer.

b. $T = \{(1, -2), (2, -1), (3, 0)\}$

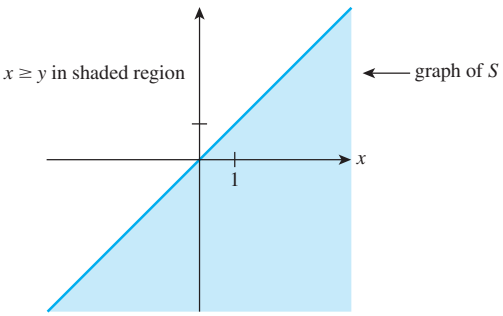
c. Domain of $T = E = \{1, 2, 3\}$, co-domain of $T = F = \{-2, -1, 0\}$

d.

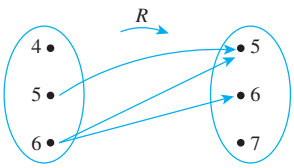


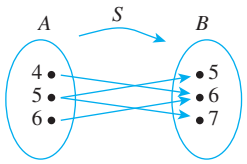
5. a. $(2, 1) \in S$ because $2 \geq 1$. $(2, 2) \in S$ because $2 \geq 2$. $2 \not S 3$ because $2 \not\geq 3$. $(-1)\ S\ (-2)$ because $-1 \geq -2$.

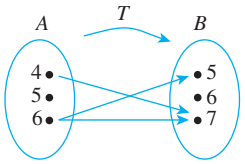
b.



7. a.







b. R is not a function because it satisfies neither property (1) nor property (2) of the definition. It fails property (1) because $(4, y) \notin R$, for any y in B. It fails property (2) because $(6, 5) \in R$ and $(6, 6) \in R$ and $5 \neq 6$.

S is not a function because $(5, 5) \in S$ and $(5, 7) \in S$ and $5 \neq 7$. So S does not satisfy property (2) of the definition of function.

T is not a function both because $(5, x) \notin T$ for any x in B and because $(6, 5) \in T$ and $(6, 7) \in T$ and $5 \neq 7$. So T does not satisfy either property (1) or property (2) of the definition of function.

9. a. There is only one: $\{(0, 1), (1, 1)\}$

b. $\{(0, 1)\}, \{(1, 1)\}$

11. $L(0201) = 4,\ L(12) = 2$

13. a. Domain $= A = \{-1, 0, 1\}$, co-domain $= B = \{t, u, v, w\}$

b. $F(-1) = u,\ F(0) = w,\ F(1) = u$

15. a. This diagram does not determine a function because 2 is related to both 2 and 6.

b. This diagram does not determine a function because 5 is in the domain but it is not related to any element in the co-domain.

16. $f(-1) = (-1)^2 = 1, f(0) = 0^2 = 0, f\left(\frac{1}{2}\right) = \left(\frac{1}{2}\right)^2 = \frac{1}{4}$.

19. For each $x \in \mathbf{R}$, $g(x) = \frac{2x^3 + 2x}{x^2 + 1} = \frac{2x(x^2 + 1)}{x^2 + 1} = 2x = f(x)$. Therefore, by definition of equality of functions, $f = g$.

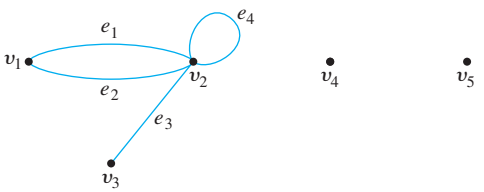
SECTION 1.4

1. $V(G) = \{v_1, v_2, v_3, v_4\}, E(G) = \{e_1, e_2, e_3\}$

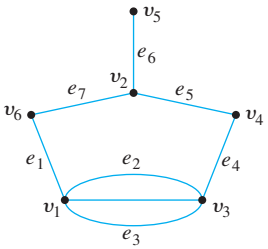
Edge-endpoint function:

Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_3\}$
e_3	$\{v_3\}$

3.



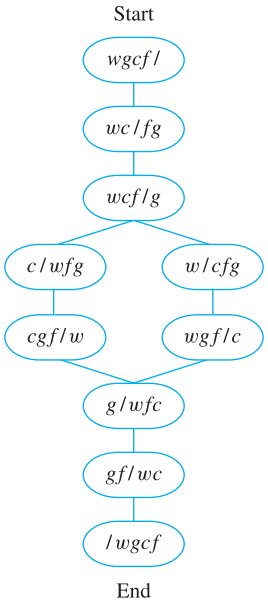
5. Imagine that the edges are strings and the vertices are knots. You can pick up the left-hand figure and lay it down again to form the right-hand figure as shown below.



8. (i) e_1, e_2, and e_3 are incident on v_1.
(ii) v_1, v_2, and v_3 are adjacent to v_3.
(iii) e_2, e_8, e_9, and e_3 are adjacent to e_1.
(iv) Loops are e_6 and e_7.
(v) e_8 and e_9 are parallel; e_4 and e_5 are parallel.
(vi) v_6 is an isolated vertex.
(vii) degree of $v_3 = 5$

10. a. Yes. According to the graph, *Sports Illustrated* is an instance of a sports magazine, a sports magazine is a periodical, and a periodical contains printed writing.

12. To solve this puzzle using a graph, introduce a notation in which, for example, *wc / fg* means that the wolf and the cabbage are on the left bank of the river and the ferryman and the goat are on the right bank. Then draw those arrangements of wolf, cabbage, goat, and ferryman that can be reached from the initial arrangement (*wgcf /*) and that are not arrangements to be avoided (such as (*wg / fc*)). At each stage ask yourself, "Where can I go from here?" and draw lines or arrows pointing to those arrangements. This method gives the graph shown below.



Examining the diagram reveals the solutions

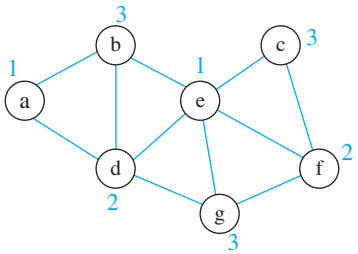
(*wgcf /*) ⟶ (*wc / gf*) ⟶ (*wcf / g*) ⟶ (*w / gcf*) ⟶
(*wgf / c*) ⟶ (*g / wcf*) ⟶ (*gf / wc*) ⟶ (*/ wgcf*)

and

(*wgcf /*) ⟶ (*wc / gf*) ⟶ (*wcf / g*) ⟶ (*c / wgf*) ⟶
(*gcf / w*) ⟶ (*g / wcf*) ⟶ (*gf / wc*) ⟶ (*/ wgcf*)

14. *Hint:* The answer is yes. Represent possible amounts of water in jugs *A* and *B* by ordered pairs. For instance, the ordered pair (1, 3) would indicate that there is one quart of water in jug *A* and three quarts in jug *B*. Starting with (0, 0), draw arrows from one ordered pair to another if it is possible to go from the situation represented by one pair to that represented by the other by either filling a jug, emptying a jug, or transferring water from one jug to another. You need only draw arrows from states that have arrows pointing to them; the other states cannot be reached. Then find a directed path (sequence of directed edges) from the initial state (0, 0) to a final state (1, 0) or (0, 1).

15.



Vertex *e* has maximal degree, so color it with color #1. Vertex *a* does not share an edge with *e*, and so color #1 may also be used for it. From the remaining uncolored vertices, all of *d*, *g*, and *f* have maximal degree. Choose any one of them—say, *d*—and use color #2 for it. Observe that vertices *c* and *f* do not share an edge with *d*, but they do share an edge with each other, which means that color #2 may be used for one but not the other. Choose to color *f* with color #2 because the degree of *f* is greater than the degree of *c*. The remaining uncolored vertices, *b*, *c*, and *g*, are unconnected, and so color #3 may be used for all three.

16. *Hint:* There are two solutions:

(1) Time 1: hiring, library
Time 2: personnel, undergraduate education, colloquium
Time 3: graduate education

(2) Time 1: hiring, library
Time 2: graduate education, colloquium
Time 3: personnel, undergraduate education

SECTION 2.1

1. Common form: If p then q.
p.
Therefore, q.
$(a+2b)(a^2-b)$ can be written in prefix notation. All algebraic expressions can be written in prefix notation.

3. Common form: $p \vee q$.
$\sim p$.
Therefore, q.
My mind is shot. Logic is confusing.

5. a. It is a statement because it is a true sentence. 1,024 is a perfect square because $1{,}024 = 32^2$, and the next smaller perfect square is $31^2 = 961$, which has fewer than four digits.

6. a. $s \wedge i$ **b.** $\sim s \wedge \sim i$

8. a. $(h \wedge w) \wedge \sim s$ **d.** $(\sim w \wedge \sim s) \wedge h$

9. a. $p \vee q$

10. a. $p \wedge q \wedge r$ **c.** $p \wedge (\sim q \vee \sim r)$

11. Inclusive or. For instance, a team could win the playoff by winning games 1, 3, and 4 and losing game 2. Such an outcome would satisfy both conditions.

12.

p	q	$\sim p$	$\sim p \wedge q$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

14.

p	q	r	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	T	F
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

16.

p	q	$p \wedge q$	$p \vee (p \wedge q)$	p
T	T	T	T	T
T	F	F	T	T
F	T	F	F	F
F	F	F	F	F

$p \vee (p \wedge q)$ and p always have the same truth values, so they are logically equivalent. (This proves one of the absorption laws.)

18.

p	t	$p \vee$ t
T	T	T
F	T	T

$p \vee$ **t** and **t** always have the same truth values, so they are logically equivalent. (This proves one of the universal bound laws.)

21.

p	q	r	$p \wedge q$	$q \wedge r$	$(p \wedge q) \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	T	F	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

$(p \wedge q) \wedge r$ and $p \wedge (q \wedge r)$ always have the same truth values, so they are logically equivalent. (This proves the associative law for $\wedge$.)

23.

p	q	r	$p \wedge q$	$q \vee r$	$(p \wedge q) \vee r$	$p \wedge (q \vee r)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	F	T	T	T
T	F	F	F	F	F	F
F	T	T	F	T	T	F
F	T	F	F	T	F	F
F	F	T	F	T	T	F
F	F	F	F	F	F	F

$(p \wedge q) \vee r$ and $p \wedge (q \vee r)$ have different truth values in the fifth and seventh rows, so they are not logically equivalent. (This proves that parentheses are needed with $\wedge$ and $\vee$.)

25. Hal is not a math major or Hal's sister is not a computer science major.

27. The connector is not loose and the machine is not unplugged.

31. a. 01, 02, 11, 12

32. $-2 \geq x$ or $x \geq 7$

34. $2 \leq x \leq 5$

36. $1 \leq x$ or $x < -3$

38. This statement's logical form is $(p \wedge q) \vee r$, so its negation has the form $\sim((p \wedge q) \vee r) \equiv \sim(p \wedge q) \wedge \sim r \equiv (\sim p \vee \sim q) \wedge \sim r$. Thus a negation for the statement is (*num_orders* $\leq$ 100 or *num_instock* $>$ 500) and *num_instock* $\geq$ 200.

40.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$p \wedge \sim q$	$\sim p \vee (p \wedge \sim q)$	$(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$
T	T	F	F	T	F	F	T
T	F	F	T	F	T	T	T
F	T	T	F	F	F	T	T
F	F	T	T	F	F	T	T

↑
Its truth values are all T's, so $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$ is a tautology.

41.

p	q	$\sim p$	$\sim q$	$p \wedge \sim q$	$\sim p \vee q$	$(p \wedge \sim q)\ (p \vee q)$
T	T	F	F	F	T	F
T	F	F	T	T	F	F
F	T	T	F	F	T	F
F	F	T	T	F	T	F

↑
Its truth values are all F's, so $(p \wedge \sim q) \wedge (\sim p \vee q)$ is a contradiction.

44. a. No real numbers satisfy this inequality

46. a. *Solution 1:* Construct a truth table for $p \oplus p$ using the truth values for *exclusive or.*

p	$p \oplus p$
T	F
F	F

because an *exclusive or* statement is false when both components are true and when both components are false.

Since all its truth values are false, $p \oplus p \equiv \mathbf{c}$, a contradiction.

Solution 2: Replace q by p in the logical equivalence $p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$, and simplify the result.

$p \oplus p \equiv (p \vee p) \wedge \sim(p \wedge p)$ by definition of $\oplus$
$\equiv p \wedge \sim p$ by the identity laws
$\equiv \mathbf{c}$ by the negation law for $\wedge$

47. There is a famous story about a philosopher who once gave a talk in which he observed that whereas in English and many other languages a double negative is equivalent to a positive, there is no language in which a double positive is equivalent to a negative. To this, another philosopher, Sidney Morgenbesser, responded sarcastically, "Yeah, yeah."

[Strictly speaking, sarcasm functions like negation. When spoken sarcastically, the words "Yeah, yeah" are not a true double positive; they just mean "no."]

48. a. The distributive law
b. The commutative law for $\vee$
c. The negation law for $\vee$
d. The identity law for $\wedge$

50. $(p \wedge \sim q) \vee p \equiv p \vee (p \wedge \sim q)$ by the commutative law for $\vee$
$\equiv p$ by the absorption law (with $\sim q$ in place of q)

53. $\sim((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \vee (p \wedge q)$

$\equiv \sim[\sim p \wedge (q \vee \sim q)] \vee (p \wedge q)$ by the distributive law

$\equiv \sim(\sim p \wedge \mathbf{t}) \vee (p \wedge q)$ by the negation law for $\vee$

$\equiv \sim(\sim p) \vee (p \wedge q)$ by the identity law for $\wedge$

$\equiv p \vee (p \wedge q)$ by the double negative law

$\equiv p$ by the absorption law

SECTION 2.2

1. If this loop does not contain a **stop** or a **go to**, then it will repeat exactly N times.

3. If you do not freeze, then I'll shoot.

5.

			conclusion	hypothesis	
p	q	$\sim p$	$\sim q$	$\sim p \vee q$	$\sim p \vee q \rightarrow \sim q$
T	T	F	F	T	F
T	F	F	T	F	T
F	T	T	F	T	F
F	F	T	T	T	T

7.

			conclusion		hypothesis	
p	q	r	$\sim q$	$p \wedge \sim q$	$p \wedge \sim q \rightarrow r$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	T	F	F	F	T
F	F	T	T	F	T
F	F	F	T	F	T

9.

p	q	r	$\sim r$	$p \wedge \sim r$	$q \vee r$	$p \wedge \sim r \leftrightarrow q \vee r$
T	T	T	F	F	T	F
T	T	F	T	T	T	T
T	F	T	F	F	T	F
T	F	F	T	T	F	F
F	T	T	F	F	T	F
F	T	F	T	F	T	F
F	F	T	F	F	T	F
F	F	F	T	F	F	T

12. If $x > 2$ then $x^2 > 4$, and if $x < -2$ then $x^2 > 4$.

13. a.

p	q	$\sim p$	$p \rightarrow q$	$\sim p \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

$p \rightarrow q$ and $\sim p \vee q$ always have the same truth values, so they are logically equivalent.

14. a. *Hint:* $p \rightarrow q \vee r$ is true in all cases except when p is true and both q and r are false.

16. Let p represent "You paid full price" and q represent "You didn't buy it at Crown Books." Thus, "If you paid full price, you didn't buy it at Crown Books" has the form $p \rightarrow q$. And "You didn't buy it at Crown Books or you paid full price" has the form $q \vee p$.

p	q	$p \rightarrow q$	$q \vee p$
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	F

These two statements are not logically equivalent because their forms have different truth values in rows 2 and 4.

(An alternative representation for the forms of the two statements is $p \rightarrow \sim q$ and $\sim q \vee p$. In this case, the truth values differ in rows 1 and 3.)

19. False. The negation of an if-then statement is not an if-then statement. It is an *and* statement.

20. a. P is a square and P is not a rectangle.

d. n is prime and both n is not odd and n is not 2.
Or: n is prime and n is neither odd nor 2.

f. Tom is Ann's father and either Jim is not her uncle or Sue is not her aunt.

21. a. Because $p \rightarrow q$ is false, p is true and q is false. Hence $\sim p$ is false, and so $\sim p \rightarrow q$ is true.

22. a. If P is not a rectangle, then P is not a square.

d. If n is not odd and n is not 2, then n is not prime.

f. If either Jim is not Ann's uncle or Sue is not her aunt, then Tom is not her father.

23. a. *Converse:* If P is a rectangle, then P is a square.
Inverse: If P is not a square, then P is not a rectangle.

d. *Converse:* If n is odd or n is 2, then n is prime.
Inverse: If n is not prime, then n is not odd and n is not 2.

f. *Converse:* If Jim is Ann's uncle and Sue is her aunt, then Tom is her father.

Inverse: If Tom is not Ann's father, then Jim is not her uncle or Sue is not her aunt.

24.

p	q	$p \to q$	$q \to p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

$p \to q$ and $q \to p$ have different truth values in the second and third rows, so they are not logically equivalent.

26.

p	q	$\sim q$	$\sim p$	$\sim q \to \sim p$	$p \to q$
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

$\sim q \to \sim p$ and $p \to q$ always have the same truth values, so they are logically equivalent.

28. *Hint:* A person who says "I mean what I say" claims to speak sincerely. A person who says "I say what I mean" claims to speak with precision.

29. $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$

p	q	r	$\sim q$	$q \vee r$	$p \wedge \sim q$	$p \to (q \vee r)$	$p \wedge \sim q \to r$	$(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$
T	T	T	F	T	F	T	T	T
T	T	F	F	T	F	T	T	T
T	F	T	T	T	T	T	T	T
T	F	F	T	F	T	F	F	T
F	T	T	F	T	F	T	T	T
F	T	F	F	T	F	T	T	T
F	F	T	T	T	F	T	T	T
F	F	F	T	F	F	T	T	T

$(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$ is a tautology because all of its truth values are T.

32. If this quadratic equation has two distinct real roots, then its discriminant is greater than zero, and if the discriminant of this quadratic equation is greater than zero, then the equation has two real roots.

34. If the Cubs do not win tomorrow's game, then they will not win the pennant.
If the Cubs win the pennant, then they will have won tomorrow's game.

37. If a new hearing is not granted, payment will be made on the fifth.

40. If I catch the 8:05 bus, then I am on time for work.

42. If this number is not divisible by 3, then it is not divisible by 9.
If this number is divisible by 9, then it is divisible by 3.

44. If Jon's team wins the rest of its games, then it will win the championship.

46. a. This statement is the converse of the given statement, and so it is not necessarily true. For instance, if the actual boiling point of compound X were 200°C, then the given statement would be true but this statement would be false.

b. This statement must be true. It is the contrapositive of the given statement.

47. a. $p \wedge \sim q \rightarrow r \equiv \sim(p \wedge \sim q) \vee r$

b. Result of $(a) \equiv \sim[\sim(\sim(p \wedge \sim q)) \wedge \sim r]$

an acceptable answer

$\equiv \sim[(p \wedge \sim q) \wedge \sim r]$

by the double negative law (another acceptable answer)

49. a. $(p \rightarrow r) \leftrightarrow (q \rightarrow r) \equiv (\sim p \vee r) \leftrightarrow (\sim q \vee r)$

$\equiv [\sim(\sim p \vee r) \vee (\sim q \vee r)] \wedge [\sim(\sim q \vee r) \vee (\sim p \vee r)]$

an acceptable answer

$\equiv [(p \wedge \sim r) \vee (\sim q \vee r)] \wedge [(q \wedge \sim r) \vee (\sim p \vee r)]$

by De Morgan's law (another acceptable answer)

b. Result of (a) $\equiv \sim[\sim(p \wedge \sim r) \wedge \sim(\sim q \vee r)] \wedge$

$\sim[\sim(q \wedge \sim r) \wedge \sim(\sim p \vee r)]$

by De Morgan's law

$\equiv \sim[\sim(p \wedge \sim r) \wedge (q \wedge \sim r)] \wedge$

$\sim[\sim(q \wedge \sim r) \wedge (p \wedge \sim r)]$

by De Morgan's law

SECTION 2.3

1. $\sqrt{2}$ is not rational. **3.** Logic is not easy.

6.

		premises		conclusion
p	q	$p \rightarrow q$	$p \rightarrow q$	$p \vee q$
T	T	T	T	T
T	F	F	T	
F	T	T	F	
F	F	T	T	F

This row shows that it is possible for an argument of this form to have true premises and a false conclusion. Thus this argument form is invalid.

7.

				premises			conclusion
p	q	r	$\sim q$	p	$p \rightarrow q$	$\sim q \vee r$	r
T	T	T	F	T	T	T	T
T	T	F	F	T	T	F	
T	F	T	T	T	F	T	
T	F	F	T	T	F	T	
F	T	T	F	F	T	T	
F	T	F	F	F	T	F	
F	F	T	T	F	T	T	
F	F	F	T	F	T	T	

This row describes the only situation in which all the premises are true. Because the conclusion is also true here, the argument form is valid.

8.

			premises				conclusion
p	q	r	$\sim q$	$p \vee q$	$p \rightarrow \sim q$	$p \rightarrow r$	r
T	T	T	F	T	F	T	
T	T	F	F	T	F	F	
T	F	T	T	T	T	T	T
T	F	F	T	T	T	F	
F	T	T	F	T	T	T	T
F	T	F	F	T	T	T	F
F	F	T	T	F	T	T	
F	F	F	T	F	T	T	

This row shows that it is possible for an argument of this form to have true premises and a false conclusion. Thus this argument form is invalid.

12. a.

		premises		conclusion
p	q	$p \rightarrow q$	q	p
T	T	T	T	T
T	F	F	F	
F	T	T	T	F
F	F	T	F	

This row shows that it is possible for an argument of this form to have true premises and a false conclusion. Thus this argument form is invalid.

14.

		premise	conclusion
p	q	p	$p \vee q$
T	T	T	T
T	F	T	T
F	T	F	
F	F	F	

These two rows show that in all situations where the premise is true, the conclusion is also true. Thus the argument form is valid.

18.

		premises		conclusion
p	q	$p \vee q$	$\sim q$	p
T	T	T	F	
T	F	T	T	T
F	T	T	F	
F	F	F	T	

This row represents the only situation in which both premises are true. Because the conclusion is also true here the argument form is valid.

22. Let p represent "Tom is on team A" and q represent "Hua is on team B." Then the argument has the form

$$\sim p \rightarrow q$$
$$\sim q \rightarrow p$$
$$\therefore \sim p \vee \sim q$$

				premises		conclusion
p	q	$\sim p$	$\sim q$	$\sim p \rightarrow q$	$\sim q \rightarrow p$	$\sim p \vee \sim q$
T	T	F	F	T	T	F
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	F	F	

This row shows that it is possible for an argument of this form to have true premises and a false conclusion. Thus this argument form is invalid.

24. $p \rightarrow q$
q
$\therefore p$ invalid: converse error

25. $p \vee q$
$\sim p$
$\therefore q$ valid: elimination

26. $p \rightarrow q$
$q \rightarrow r$
$\therefore p \rightarrow r$ valid: transitivity

27. $p \rightarrow q$
$\sim p$
$\therefore \sim q$ invalid: inverse error

36. The program contains an undeclared variable.
One explanation:

1. There is not a missing semicolon and there is not a misspelled variable name. *(by (c) and (d) and definition of $\wedge$)*
2. It is not the case that there is a missing semicolon or a misspelled variable name. *(by (1) and De Morgan's laws)*
3. There is not a syntax error in the first five lines. *(by (b) and (2) and modus tollens)*
4. There is an undeclared variable. *(by (a) and (3) and elimination)*

37. The treasure is buried under the flagpole.
One explanation:

1. The treasure is not in the kitchen. *(by (c) and (a) and modus ponens)*
2. The tree in the front yard is not an elm. *(by (b) and (1) and modus tollens)*
3. The treasure is buried under the flagpole. *(by (d) and (2) and elimination)*

38. a. A is a knave and B is a knight.
One explanation:

1. Suppose A is a knight.
2. $\therefore$ What A says is true. *(by definition of knight)*
3. $\therefore$ B is a knight also. *(That's what A said.)*
4. $\therefore$ What B says is true. *(by definition of knight)*
5. $\therefore$ A is a knave. *(That's what B said.)*
6. $\therefore$ We have a contradiction: A is a knight and a knave. *(by (1) and (5))*
7. $\therefore$ The supposition that A is a knight is false. *(by the contradiction rule)*
8. $\therefore$ A is a knave. *(negation of supposition)*
9. $\therefore$ What B says is true. *(B said A was a knave, which we now know to be true.)*
10. $\therefore$ B is a knight. *(by definition of knight)*

d. *Hint:* W and Y are knights; the rest are knaves.

39. The chauffeur killed Lord Hazelton.
One explanation:

1. Suppose the cook was in the kitchen at the time of the murder.
2. $\therefore$ The butler killed Lord Hazelton with strychnine. *(by (c) and (1) and modus ponens)*
3. $\therefore$ We have a contradiction: Lord Hazelton was killed by strychnine and a blow on the head. *(by (2) and (a))*
4. $\therefore$ The supposition that the cook was in the kitchen is false. *(by the contradiction rule)*
5. $\therefore$ The cook was not in the kitchen at the time of the murder. *(negation of supposition)*
6. $\therefore$ Sara was not in the dining room when the murder was committed. *(by (e) and (5) and modus ponens)*
7. $\therefore$ Lady Hazelton was in the dining room when the murder was committed. *(by (b) and (6) and elimination)*
8. $\therefore$ The chauffeur killed Lord Hazelton. *(by (d) and (7) and modus ponens)*

41.

(1)	$p \rightarrow t$	by premise (d)
	$\sim p$	by premise (c)
	$\therefore \sim p$	by modus tollens
(2)	$\sim p$	by (1)
	$\therefore \sim p \vee q$	by generalization
(3)	$\sim p \vee q \rightarrow r$	by premise (a)
	$\sim p \vee q$	by (2)
	$\therefore r$	by modus ponens
(4)	$\sim p$	by (1)
	r	by (3)
	$\therefore \sim p \wedge r$	by conjunction
(5)	$\sim p \wedge r \rightarrow \sim s$	by premise (e)
	$\sim p \wedge r$	by (4)
	$\therefore \sim s$	by modus ponens
(6)	$s \vee \sim q$	by premise (b)
	$\sim s$	by (5)
	$\therefore \sim q$	by elimination

43. (1) $\sim w$ by premise (d)
$u \vee w$ by premise (e)
$\therefore u$ by elimination
(2) $u \rightarrow \sim p$ by premise (c)
u by (1)
$\therefore \sim p$ by modus ponens
(3) $\sim p \rightarrow r \wedge \sim s$ by premise (a)
$\sim p$ by (2)
$\therefore r \wedge \sim s$ by modus ponens
(4) $r \wedge \sim s$ by (3)
$\therefore \sim s$ by specialization
(5) $\sim t \rightarrow s$ by premise (b)
$\sim s$ by (4)
$\therefore \sim t$ by modus tollens

SECTION 2.4

1. $R = 1$ **3.** $S = 1$

5.

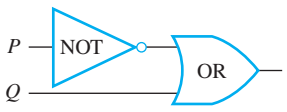
Input		Output
P	***Q***	***R***
1	1	1
1	0	1
0	1	0
0	0	1

7.

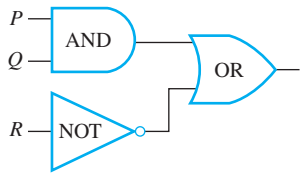
Input			Output
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

9. $P \vee \sim Q$ **11.** $(P \wedge \sim Q) \vee R$

13.

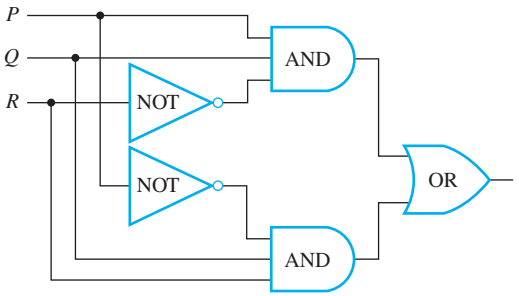


16.



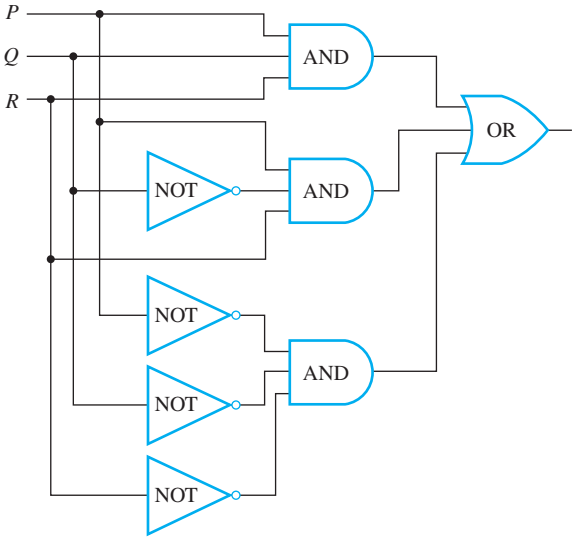
18. a. $(P \wedge Q \wedge \sim R) \vee (\sim P \wedge Q \wedge R)$

b.



20. a. $(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (\sim P \wedge \sim Q \wedge \sim R)$

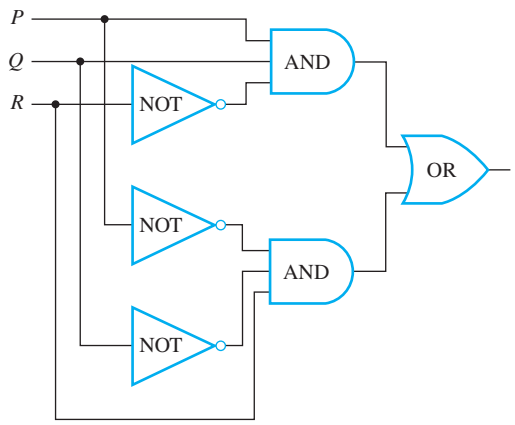
b.



22. The input/output table is

Input			Output
P	***Q***	***R***	***S***
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

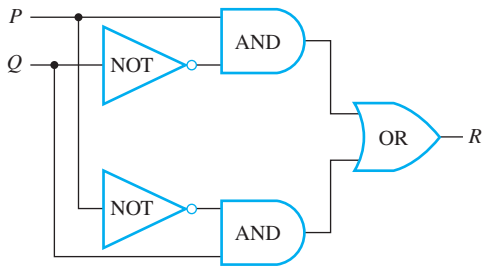
One circuit (among many) having this input/output table is shown below.



24. Let P and Q represent the positions of the switches in the classroom, with 0 being "down" and 1 being "up." Let R represent the condition of the light, with 0 being "off" and 1 being "on." Initially, $P = Q = 0$ and $R = 0$. If either P or Q (but not both) is changed to 1, the light turns on. So when $P = 1$ and $Q = 0$, then $R = 1$, and when $P = 0$ and $Q = 1$, then $R = 1$. Thus when one switch is up and the other is down the light is on, and hence moving the switch that is down to the up position turns the light off. So when $P = 1$ and $Q = 1$, then $R = 0$. It follows that the input/output table has the following appearance:

Input		Output
P	***Q***	***R***
1	1	0
1	0	1
0	1	1
0	0	0

One circuit (among many) having this input/output table is the following:



26. The Boolean expression for (a) is $(P \wedge Q) \vee Q$, and for (b) it is $(P \vee Q) \wedge Q$. We must show that if these expressions are regarded as statement forms, then they are logically equivalent. Now

$(P \wedge Q) \vee Q$

$\equiv Q \vee (P \wedge Q)$ by the commutative law for $\vee$

$\equiv (Q \vee P) \wedge (Q \vee Q)$ by the distributive law

$\equiv (Q \vee P) \wedge Q$ by the idempotent law

$\equiv (P \vee Q) \wedge Q$ by the commutative law for $\wedge$

Alternatively, by the absorption laws, both statement forms are logically equivalent to Q.

30. $(P \wedge Q) \vee (\sim P \wedge Q) \vee (\sim P \wedge \sim Q)$

$\equiv (P \wedge Q) \vee ((\sim P \wedge Q) \vee (\sim P \wedge \sim Q))$ by inserting parentheses (which is legal by the associative law)

$\equiv (P \wedge Q) \vee (\sim P \wedge (Q \vee \sim Q))$ by the distributive law

$\equiv (P \wedge Q) \vee (\sim P \wedge \mathbf{t})$ by the negation law for $\vee$

$\equiv (P \wedge Q) \vee \sim P$ by the identity law for $\wedge$

$\equiv \sim P \vee (P \wedge Q)$ by the commutative law for $\vee$

$\equiv (\sim P \vee P) \wedge (\sim P \vee Q)$ by the distributive law

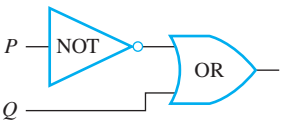
$\equiv (P \vee \sim P) \wedge (\sim P \vee Q)$ by the commutative law for $\vee$

$\equiv \mathbf{t} \wedge (\sim P \vee Q)$ by the negation law for $\vee$

$\equiv (\sim P \vee Q) \wedge \mathbf{t}$ by the commutative law for $\wedge$

$\equiv \sim P \vee Q$ by the identity law for $\wedge$

The following is, therefore, a circuit with at most two logic gates that has the same input/output table as the circuit corresponding to the given expression.



34. b. $(P \downarrow Q) \downarrow (P \downarrow Q)$

$\equiv \sim(P \downarrow Q)$ by part (a)

$\equiv \sim[\sim(P \vee Q)]$ by definition of $\downarrow$

$\equiv P \vee Q$ by the double negative law

d. *Hint:* Use the results of exercise 13 of Section 2.2 and part (a) and (c) of this exercise.

SECTION 2.5

1. $19_{10} = 16 + 2 + 1 = 10011_2$

4. $458_{10} = 256 + 128 + 64 + 8 + 2 = 111001010_2$

7. $1110_2 = 8 + 4 + 2 = 14_{10}$

10. $1100101_2 = 64 + 32 + 4 + 1 = 101_{10}$

13.

$$\begin{array}{cccccc} & \overset{1}{1} & \overset{1}{0} & \overset{1}{1} & 1_2 \\ + & & 1 & 0 & 1_2 \\ \hline 1 & 0 & 0 & 0 & 0_2 \end{array}$$

15.
$$\begin{array}{rcccccc} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & {\scriptstyle 1} & \\ & 1 & 0 & 1 & 1 & 0 & 1_2 \\ + & & 1 & 1 & 1 & 0 & 1_2 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 0_2 \end{array}$$

17.
$$\begin{array}{rcccc} & & {\scriptstyle 1} & & \\ & {\scriptstyle 1} & {\scriptstyle 10} & {\scriptstyle \not{1}\not{0}} & {\scriptstyle 1} \\ 1 & \not{0} & \not{1} & 0 & 0_2 \\ - & 1 & 1 & 0 & 1_2 \\ \hline & & 1 & 1 & 1_2 \end{array}$$

19.
$$\begin{array}{rcccccc} & & & {\scriptstyle 0} & {\scriptstyle \not{1}\not{0}} & & \\ 1 & 0 & 1 & \not{1} & 0 & 1_2 \\ - & 1 & 0 & 0 & 1 & 1_2 \\ \hline & 1 & 1 & 0 & 1 & 0_2 \end{array}$$

21. a. $S = 0, T = 1$

23. $|-23|_{10} = 23_{10} = (16+4+2+1)_{10} = 00010111_2$ $\xrightarrow{\text{flip the bits}}$ 11101000 $\xrightarrow{\text{add 1}}$ 11101001. So the answer is 11101001.

25. $|-4|_{10} = 4_{10} = 00000100_2 \xrightarrow{\text{flip the bits}} 11111011$ $\xrightarrow{\text{add 1}}$ 11111100. So the answer is 11111100.

27. Because the leading bit is 1, this is the 8-bit two's complement of a negative integer. 11010011 $\xrightarrow{\text{flip the bits}}$ 00101100 $\xrightarrow{\text{add 1}}$ $00101101_2 =$ $(32+8+4+1)_{10} = |-45|_{10}$. So the answer is -45.

29. Because the leading bit is 1, this is the 8-bit two's complement of a negative integer. 11110010 $\xrightarrow{\text{flip the bits}}$ 00001101 $\xrightarrow{\text{add 1}}$ $00001110_2 =$ $(8+4+2)_{10} = |-14|_{10}$. So the answer is -14.

31. $57_{10} = (32+16+8+1)_{10} = 111001_2 \rightarrow 00111001$
$|-118|_{10} = (64+32+16+4+2)_{10} = 01110110_2$
$\xrightarrow{\text{flip the bits}}$ 10001001 $\xrightarrow{\text{add 1}}$ 10001010. So the 8-bit two's complements of 57 and -118 are 00111001 and 10001010. Adding the 8-bit two's complements in binary notation gives

+	0	0	1	1	1	0	0	1
	1	0	0	0	1	0	1	0
	1	1	0	0	0	0	1	1

Since the leading bit of this number is a 1, the answer is negative. Converting back to decimal form gives

$11000011 \xrightarrow{\text{flip the bits}} 00111100 \xrightarrow{\text{add 1}} 00111101_2$
$= (32+16+8+4+1)_{10} = |61|_{10}$.

So the answer is -61.

32. $62_{10} = (32+16+8+4+2)_{10}$
$= 111110_2 \rightarrow 00111110$
$|-18|_{10} = (16+2)_{10} = 00010010$
$\xrightarrow{\text{flip the bits}}$ 11101101
$\xrightarrow{\text{add 1}}$ 11101110

Thus the 8-bit two's complements of 62 and -18 are 00111110 and 10110111. Adding the 8-bit two's complements in binary notation gives

+	0	0	1	1	1	1	1	0
	1	1	1	0	1	1	1	0
1	0	0	1	0	1	1	0	0

Truncating the 1 in the 2^8th position gives 00101100. Since the leading bit of this number is a 0, the answer is positive. Converting back to decimal form gives

$00101100 \rightarrow 101100_2 = (32+8+4)_{10} = 44_{10}$.

So the answer is 44.

33. $|-6|_{10} = (4+2)_{10}$
$= 110_2 \xrightarrow{\text{flip the bits}} 00000110 \rightarrow$
$11111001 \xrightarrow{\text{add 1}} 11111010$
$|-73|_{10} = (64+8+1)_{10}$
$= 01001001 \xrightarrow{\text{flip the bits}}$
$10110110 \xrightarrow{\text{add 1}} 10110111$

Thus the 8-bit two's complements of -6 and -73 are 11111010 and 10110111. Adding the 8-bit two's complements in binary notation gives

+	1	1	1	1	1	0	1	0
	1	0	1	1	0	1	1	1
1	1	0	1	1	0	0	0	1

Truncating the 1 in the 2^8th position gives 10110001. Since the leading bit of this number is a 1, the answer is negative. Converting back to decimal form gives

$10110001 \xrightarrow{\text{flip the bits}} 01001110 \xrightarrow{\text{add 1}} 01001111_2$
$= (64+8+4+2+1) = 79_{10} = |-79|_{10}$

So the answer is -79.

37. a. The 8-bit two's complement of -128 is computed as follows:

$|-128|_{10} = 128_{10} = (2^7)_{10}$
$= 10000000_2 \xrightarrow{\text{flip the bits}} 01111111 \xrightarrow{\text{add 1}} 10000000.$

So the 8-bit two's complement of -128 is 10000000. If the two's complement procedure is applied to this result, the following is obtained

$$10000000 \xrightarrow{\text{flip the bits}} 01111111 \xrightarrow{\text{add 1}} 10000000.$$

So the 8-bit two's complement of the 8-bit two's complement of -128 is 10000000, which is the 8-bit two's complement of -128.

38. $A2BC_{16} = 10\cdot16^3 + 2\cdot16^2 + 11\cdot16 + 12 = 41{,}660_{10}$

41. $000111000000101010111110_2$

44. $2E_{16}$

47. a. $6\cdot8^4 + 1\cdot8^3 + 5\cdot8^2 + 0\cdot8 + 2\cdot1 = 25{,}410_{10}$

SECTION 3.1

1. a. False **b.** True

2. a. The statement is true. The integers correspond to certain of the points on a number line, and the real numbers correspond to all the points on the number line.

b. The statement is false; 0 is neither positive nor negative.

c. The statement is false. For instance, let $r = -2$. Then $-r = -(-2) = 2$, which is positive.

d. The statement is false. For instance, the number $\frac{1}{2}$ is a real number, but it is not an integer.

3. a. When $m = 25$ and $n = 10$, the statement "m is a factor of n^2" is true because $n^2 = 100$ and $100 = 4\cdot25$. But the statement "m is a factor of n" is false because 10 is not a product of 25 times any integer. Thus the hypothesis of $R(m, n)$ is true and the conclusion is false, so the statement as a whole is false.

c. When $m = 5$ and $n = 10$, both statements "m is a factor of n^2" and "m is a factor of n" are true because $n = 10 = 5\cdot20 = m\cdot20$. Thus both the hypothesis and conclusion of $R(m, n)$ are true, and so the statement as a whole is true.

4. a. $Q(-2, 1)$ is the statement "If $-2 < 1$ then $(-2)^2 < 1^2$." The hypothesis of this statement is $-2 < 1$, which is true. The conclusion is $(-2)^2 < 1^2$, which is false because $(-2)^2 = 4$ and $1^2 = 1$ and $4 \not< 1$. Thus $Q(-2, 1)$ is a conditional statement with a true hypothesis and a false conclusion. So $Q(-2, 1)$ is false.

c. $Q(3, 8)$ is the statement "If $3 < 8$ then $3^2 < 8^2$." The hypothesis of this statement is $3 < 8$, which is true. The conclusion is $3^2 < 8^2$, which is also true because $3^2 = 9$ and $8^2 = 64$ and $9 < 64$. Thus $Q(3, 8)$ is a conditional statement with a true hypothesis and a true conclusion. So $Q(3, 8)$ is true.

5. a. The truth set is the set of all integers d such that $6/d$ is an integer, so the truth set is $\{-6, -3, -2, -1, 1, 2, 3, 6\}$.

c. The truth set is the set of all real numbers x with the property that $1 \le x^2 \le 4$, so the truth set is $\{x \in \mathbf{R} \mid -2 \le x \le -1 \text{ or } 1 \le x \le 2\}$. In other words, the truth set is the set of all real numbers between -2 and -1 inclusive together with those between 1 and 2 inclusive.

6. a. $\{-9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

7. *baa, bab, bac, bba, bbb, bbc, bca, bcb*

9. Counterexample: Let $x = 1/2$. Then $\frac{1}{x} = \frac{1}{(1/2)} = 2$, and $1/2 \not> 2$. (*This is one counterexample among many.*)

11. Counterexample: Let $m = 1$ and $n = 1$. Then $m\cdot n = 1\cdot1 = 1$ and $m + n = 1 + 1 = 2$. But $1 \not> 2$, and so $m\cdot n \not> m + n$. (*This is one counterexample among many.*)

13. (a), (e), (f) **14.** (b), (c), (e), (f)

15. a. *Partial answer:* Every rectangle is a quadrilateral.

b. *Partial answer:* At least one set has 16 subsets.

16. a. $\forall$ dinosaur x, x is extinct.

c. $\forall$ irrational number x, x is not an integer.

e. $\forall$ integer x, x^2 does not equal 2, 147, 581, 953.

17. a. $\exists$ an exercise x such that x has an answer.

18. a. $\exists s \in D$ such that $E(s)$ and $M(s)$. (*Or:* $\exists s \in D$ such that $E(s) \wedge M(s)$.)

b. $\forall s \in D$, if $C(s)$ then $E(s)$. (*Or:* $\forall s \in D$, $C(s) \rightarrow E(s)$.)

e. ($\exists s \in D$ such that $C(s) \wedge E(s)$) $\wedge$ ($\exists s \in D$ such that $C(s) \wedge \sim E(s)$)

19. (b), (d), (e)

20. *Partial answer:* The square root of a positive real number is positive.

21. a. The total degree of G is even, for any graph G.

c. p is even, for some prime number p.

22. a. $\forall x$, if x is a Java program, then x has at least 5 lines.

23. a. $\forall x$ if x is an equilateral triangle, then x is isosceles.
$\forall$ equilateral triangles x, x is isosceles.

24. a. $\exists$ a hatter x such that x is mad.
$\exists x$ such that x is a hatter and x is mad.

25. a. $\forall$ nonzero fraction x, the reciprocal of x is a fraction.
$\forall x$, if x is a nonzero fraction then the reciprocal of x is a fraction.

c. $\forall$ triangle x, the sum of the angles of x is 180°. $\forall x$, if x is a triangle then the sum of the angles of x is 180°.

e. $\forall$ even integers x and y, the sum of x and y is even.
$\forall x$ and y, if x and y are even integers then the sum of x and y is even.

26. b. $\forall x(\text{Int}(x) \rightarrow \text{Ratl}(x)) \wedge \exists x(\text{Ratl}(x) \wedge \sim\text{Int}(x))$

27. a. False. Figure b is a circle that is not gray.

b. True. All the gray figures are circles.

28. b. *One answer among many:* If a real number is negative, then when its opposite is computed, the result is a positive real number.

This statement is true because for each real number x, $-(-|x|) = |x|$ (and any negative real number can be represented as $-|x|$, for some real number x).

d. *One answer among many:* There is a real number that is not an integer. This statement is true. For instance, $\frac{1}{2}$ is a real number that is not an integer.

30. b. *One answer among many:* If an integer is prime, then it is not a perfect square.

This statement is true because a prime number is an integer greater than 1 that is not a product of two smaller positive integers. So a prime number cannot be a perfect square because if it were, it would be a product of two smaller positive integers.

31. *Hint:* Your answer should have the appearance shown in the following made-up example:

Statement: "If a function is differentiable, then it is continuous."

Formal version: $\forall$ function f, if f is differentiable, then f is continuous.

Citation: Calculus by D. R. Mathematician, Best Publishing Company, 2019, page 263.

32. a. True: Any real number that is greater than 2 is greater than 1.

c. False: $(-3)^2 > 4$ but $-3 \not> 2$.

33. a. True. Whenever both a and b are positive, so is their product.

b. False. Let $a = -2$ and $b = -3$. Then $ab = 6$, which is not less than zero.

SECTION 3.2

1. (a) and (e) are negations.

3. a. $\exists$ a string s such that s does not have any characters. (*Or:* $\exists$ a string s such that s has no characters.)

c. $\forall$ movie m, m is less than or equal to 6 hours long. (*Or:* $\forall$ movie m, m is no more than 6 hours long.)

In 4–6 there are other correct answers in addition to those shown.

4. a. Some dogs are unfriendly. (*Or:* There is at least one unfriendly dog.)

c. All suspicions were unsubstantiated. (*Or:* No suspicions were substantiated.)

5. a. There is a valid argument that does not have a true conclusion. (*Or:* There is at least one valid argument that does not have a true conclusion.)

6. a. Sets A and B have at least one point in common.

7. a. This vertex is connected to at least one other vertex in the graph. (*Or:* There is at least one other vertex in the graph to which this vertex is connected.) (*Or:* This vertex is connected to some other vertex in the graph.)

9. $\exists$ a real number x such that $x > 3$ and $x^2 \leq 9$.

11. The proposed negation is not correct. The given statement makes a claim about *any* two irrational numbers and means that no matter what two irrational numbers you might choose, the sum of those numbers will be irrational. For this to be false means that there is at least one pair of irrational numbers whose sum is rational. On the other hand, the negation proposed in the exercise ("The sum of any two irrational numbers is rational") means that given *any* two irrational numbers, their sum is rational. This is a much stronger statement than the actual negation: The truth of this statement implies the truth of the negation (assuming that there are at least two irrational numbers), but the negation can be true without having this statement be true.

Correct negation: There are at least two irrational numbers whose sum is rational.

Or: The sum of some two irrational numbers is rational.

13. The proposed negation is not correct. There are two mistakes: The negation of a "for every" statement is not a "for every" statement; and the negation of an if-then statement is not an if-then statement.

Correct negation: There exists an integer n such that n^2 is even and n is not even.

15. a. True: All the odd numbers in D are positive.

c. False: $x = 16$, $x = 26$, $x = 32$, and $x = 36$ are all counterexamples.

16. $\exists$ a real number x such that $x^2 \geq 1$ and $x \not> 0$. In other words, $\exists$ a real number x such that $x^2 \geq 1$ and $x \leq 0$.

18. $\exists$ a real number x such that $x(x+1) > 0$ and both $x \leq 0$ and $x \geq -1$.

20. $\exists$ integers a, b, and c such that $a - b$ is even and $b - c$ is even and $a - c$ is not even.

22. There is an integer with the property that the square of the integer is odd but the integer itself is not odd. (*Or:* At least one integer has an odd square but is not itself odd.)

24. a. If a person is a child in Tom's family, then the person is female.

If a person is a female in Tom's family, then the person is a child.

The second statement is the converse of the first.

25. a. *Converse:* If $n + 1$ is an even integer, then n is a prime number that is greater than 2.

Counterexample: Let $n = 15$. Then $n + 1 = 16$, which is even but n is not a prime number that is greater than 2.

26. *Statement:* $\forall$ real number x, if $x^2 \geq 1$ then $x > 0$.

Contrapositive: $\forall$ real number x, if $x \leq 0$ then $x^2 < 1$.

Converse: $\forall$ real number x, if $x > 0$ then $x^2 \geq 1$.

Inverse: $\forall$ real number x, if $x^2 < 1$ then $x \leq 0$.

The statement and its contrapositive are false. As a counterexample, let $x = -2$. Then $x^2 = (-2)^2 = 4$, and so $x^2 \geq 1$. However $x \not> 0$.

The converse and the inverse are also false. As a counterexample, let $x = 1/2$. Then $x^2 = 1/4$, and so $x > 0$ but $x^2 \not\geq 1$.

28. *Statement:* $\forall x \in \mathbf{R}$, if $x(x+1) > 0$ then $x > 0$ or $x < -1$.

Contrapositive: $\forall x \in \mathbf{R}$, if $x \leq 0$ and $x \geq -1$, then $x(x+1) \leq 0$.

Converse: $\forall x \in \mathbf{R}$, if $x > 0$ or $x < -1$ then $x(x+1) > 0$.

Inverse: $\forall x \in \mathbf{R}$, if $x(x+1) \leq 0$ then $x \leq 0$ and $x \geq -1$.

The statement, its contrapositive, its converse, and its inverse are all true.

30. *Statement:* $\forall$ integers a, b, and c, if $a - b$ is even and $b - c$ is even, then $a - c$ is even.

Contrapositive: $\forall$ integers a, b, and c, if $a - c$ is not even, then $a - b$ is not even or $b - c$ is not even.

Converse: $\forall$ integers a, b, and c, if $a - c$ is even then $a - b$ is even and $b - c$ is even.

Inverse: $\forall$ integers a, b, and c, if $a - b$ is not even or $b - c$ is not even, then $a - c$ is not even.

The statement is true, but its converse and inverse are false. As a counterexample, let $a = 3$, $b = 2$, and $c = 1$. Then $a - c = 2$, which is even, but $a - b = 1$ and $b - c = 1$, so it is not the case that both $a - b$ and $b - c$ are even.

32. *Statement:* If the square of an integer is odd, then the integer is odd.

Contrapositive: If an integer is not odd, then the square of the integer is not odd.

Converse: If an integer is odd, then the square of the integer is odd.

Inverse: If the square of an integer is not odd, then the integer is not odd.

The statement, its contrapositive, its converse, and its inverse are all true.

34. a. If n is divisible by some prime number between 1 and $\sqrt{n}$ inclusive, then n is not prime.

36. a. *One possible answer:* Let $P(x)$ be "$2x \neq 1$." The statement "$\forall x \in \mathbf{Z}$, $2x \neq 1$" is true because there is no integer which, when doubled, equals 1. But the statements "$\forall x \in \mathbf{Q}$, $2x \neq 1$" and "$\forall x \in \mathbf{R}$, $2x \neq 1$" are both false because $x = 1/2$ satisfies the equation $2x = 1$ and 1/2 is in both $\mathbf{R}$ and $\mathbf{Q}$.

37. The claim is "$\forall x$, if $x = 1$ and x is in the sequence 0204, then x is to the left of all the 0's in the sequence."

The negation is "$\exists x$ such that $x = 1$ and x is in the sequence 0204, and x is not to the left of all the 0's in the sequence." The negation is false because the sequence does not contain the character 1. So the claim is vacuously true (or true by default).

39. If a person earns a grade of C$^-$ in this course, then the course counts toward graduation.

41. If a person is not on time each day, then the person will not keep this job.

43. If a number is prime, then it is greater than 1.

45. To say that "Being divisible by 8 is a necessary condition for being divisible by 4" means that, "If a number is not divisible by 8 then that number is not divisible by 4. The negation is, "There is a number that is not divisible by 8 and is divisible by 4."

47. To say that "having a large income is a sufficient condition for being happy" means that "If a person has a large income then that person is happy." The negation is "There is a person who has a large income and is not happy."

50. No. Interpreted formally, the statement says, "If carriers do not offer the same lowest fare, then you may not select among them."

SECTION 3.3

1. a. True: Tokyo is the capital of Japan.
b. False: Athens is not the capital of Egypt.

2. a. True: $2^2 > 3$
b. False: $1^2 \not> 1$

3. a. $y = \frac{1}{2}$
b. $y = -1$

4. a. Let $n = 16$. Then $n > x$ because $16 > 15.83$.

5. The statement says that no matter what circle anyone might give you, you can find a square of the same color.

Solution 1: The statement is true because the only circles in the Tarski world are a, b, and c, and given a or c, which are blue, square j is also blue, and given b, which is gray, squares g and h are also gray.

Solution 2: The statement is true. The Tarski world has exactly three circles: a, b, and c.

Given circle $x =$	Choose square $y =$	Is y the same color as x?
a	j	yes ✓
b	g or h	yes ✓
c	j	yes ✓

7. *Solution 1:* The statement is true because the Tarski world has exactly four squares: e, g, h, and j and triangle d is above all of them.

Solution 2: The statement is true. The Tarski world has exactly four squares: e, g, h, and j.

Choose triangle $x = d$	Choose square $y =$	Is x above y?
	e	yes ✓
	f	yes ✓
	h	yes ✓
	j	yes ✓

9. a. There are five elements in D. For each, an element in E must be found so that the sum of the two equals 0. So: for $x = -2$, take $y = 2$; for $x = -1$, take $y = 1$; for $x = 0$, take $y = 0$;for $x = 1$, take $y = -1$; and for $x = 2$, take $y = -2$.

Alternatively, note that for each integer x in D, the integer $-x$ is also in D, including 0 (because $-0 = 0$), and for every integer x, $x + (-x) = 0$.

10. a. True. Every student chose at least one dessert: Uta chose pie, Tim chose both pie and cake, and Yuen chose pie.
c. This statement says that some particular dessert was chosen by every student. This is true: Every student chose pie.

11. a. There is a student who has seen *Casablanca*.
c. Every student has seen at least one movie.
d. There is a movie that has been seen by every student. (There are many other acceptable ways to state these answers.)

12. a. *Negation:* $\exists x$ in D such that $\forall y$ in E, $x + y \neq 1$.

The negation is true. When $x = -2$, the only number y with the property that $x + y = 1$ is $y = 3$, and 3 is not in E.

b. *Negation:* $\forall x$ in D, $\exists y$ in E such that $x + y \neq -y$.

The negation is true because the original statement is false. To see that the original statement is false, take any x in D and choose y to be any number in E with $y \neq -\frac{x}{2}$. Then $2y \neq -x$, and adding x and subtracting y from both sides gives $x + y \neq -y$.

In 13–19 there are other correct answers in addition to those shown.

13. a. *Statement:* For every color, there is an animal of that color.
There are animals of every color.
b. *Negation:* $\exists$ a color C such that $\forall$ animal A, A is not colored C.
For some color, there is no animal of that color.

14. a. *Statement:* There is a book that every person has read.
b. *Negation:* There is no book that every person has read.
(*Or:* $\forall$ book b, $\exists$ a person p such that p has not read b.)

15. a. *Statement:* For every odd integer n, there is an integer k such that $n = 2k + 1$.

Given any odd integer, there is another integer for which the given integer equals twice the other integer plus 1. Given any odd integer n, we can find another integer k so that $n = 2k + 1$.

An odd integer is equal to twice some other integer plus 1.

Every odd integer has the form $2k + 1$ for some integer k.

b. *Negation:* $\exists$ an odd integer n such that $\forall$ integer k, $n \neq 2k + 1$.

There is an odd integer that is not equal to $2k + 1$ for any integer k.

Some odd integer does not have the form $2k + 1$ for any integer k.

18. a. *Statement:* For every real number x, there is a real number y such that $x + y = 0$.

Given any real number x, there exists a real number y such that $x + y = 0$.

Given any real number, we can find another real number (possibly the same) such that the sum of the given number plus the other number equals 0.

Every real number can be added to some other real number (possibly itself) to obtain 0.

b. *Negation:* $\exists$ a real number x such that $\forall$ real number y, $x + y \neq 0$.

There is a real number x for which there is no real number y with $x + y = 0$.

There is a real number x with the property that $x + y \neq 0$ for any real number y.

Some real number has the property that its sum with any other real number is nonzero.

20. a. Statement (1) says that no matter what square anyone might give you, you can find a triangle of a different color. This is true because the only squares are e, g, h, and j, and given squares g and h, which are gray, you could take triangle d, which is black; given square e, which is black, you could take either triangle f or i, which are gray; and given square j, which is blue, you could take either triangle f or h, which are gray, or triangle d, which is black. In each case the chosen triangle has a different color from the given square.

21. a. (1) The statement "$\forall$ real number x, $\exists$ a real number y such that $2x + y = 7$" is true. Given any real number x, take y to be $7 - 2x$.

(2) The statement "$\exists$ a real number x such that $\forall$ real number y, $2x + y = 7$" is false. If it were true, the single number x would equal $\frac{7 - y}{2}$ for every real number y, and that is impossible.

b. Both statements (1) "$\forall$ real number x, $\exists$ a real number y such that $x + y = y + x$" and (2) "$\exists$ a real number x such that $\forall$ real number y, $x + y = y + x$" are true.

22. a. Given any real number, you can find a real number so that the sum of the two is zero. In other words, every real number has an additive inverse. This statement is true.

b. There is a real number with the following property: No matter what real number is added to it, the sum of the two will be zero. In other words, there is one particular real number whose sum with any real number is zero. This statement is false; no one number will work for all numbers. For instance, if $x + 0 = 0$, then $x = 0$, but in that case $x + 1 = 1 \neq 0$.

24. a. $\sim(\forall x \in D(\forall y \in E(P(x, y))))$

$\equiv \exists x \in D(\sim(\forall y \in E(P(x, y))))$

$\equiv \exists x \in D(\exists y \in E(\sim P(x, y)))$

25. This statement says that all of the circles are above all of the squares. This statement is true because the circles are a, b, and c, and the squares are e, g, h, and j, and all of a, b, and c lie above all of e, g, h, and j.

Negation: There is a circle x and a square y such that x is not above y. In other words, at least one of the circles is not above at least one of the squares.

27. The statement says that there are a circle and a square with the property that the circle is above the square and has a different color from the square. This statement is true. For example, circle a lies above square e and is differently colored from e. (Several other examples could also be given.)

29. a. *Version with interchanged quantifiers:* $\exists x \in \mathbf{R}$ such that $\forall y \in \mathbf{R}$, $x < y$.

b. The given statement says that for any real number x, there is a real number y that is greater than x. This is true: For any real number x, let $y = x + 1$. Then $x < y$. The version with interchanged quantifiers says that there is a real number that is less than every other real number (including the negative ones). This is false.

31. $\forall$ person x, $\exists$ a person y such that x is older than y.

32. $\exists$ a person x such that $\forall$ person y, x is older than y.

33. a. *Formal version:* $\forall$ person x, $\exists$ a person y such that x loves y.

b. *Negation:* $\exists$ a person x such that $\forall$ person y, x does not love y. In other words, there is someone who does not love anyone.

34. a. *Formal version:* $\exists$ a person x such that $\forall$ person y, x loves y.

b. *Negation:* $\forall$ person x, $\exists$ a person y such that x does not love y. In other words, everyone has someone whom they do not love.

37. a. *Statement:* $\forall$ even integer n, $\exists$ an integer k such that $n = 2k$.

b. *Negation:* $\exists$ an even integer n such that $\forall$ integer k, $n \neq 2k$.

There is some even integer that is not equal to twice any other integer.

39. a. *Statement:* $\exists$ a program P such that $\forall$ question Q posed to P, P gives the correct answer to Q.

b. *Negation:* $\forall$ program P, there is a question Q that can be posed to P such that P does not give the correct answer to Q.

40. a. $\forall$ minutes m, $\exists$ a sucker s such that s was born in minute m.

41. a. This statement says that given any positive integer, there is a positive integer such that the first integer is 1 more than the second integer. This is false. Given the positive integer $x = 1$, the only integer with the property that $x = y + 1$ is $y = 0$, and 0 is not a positive integer.

b. This statement says that given any integer, there is an integer such that the first integer is 1 more than the second integer. This is true. Given any integer x, take $y = x - 1$. Then y is an integer, and $y + 1 = (x - 1) + 1 = x$.

e. This statement says that given any real number, there is a real number such that the product of the two is equal to 1. This is false because $0 \cdot y = 0 \neq 1$ for every number y. So when $x = 0$, there is no real number y with the property that $xy = 1$.

f. This statement is true because the real number 0 has the property that $\forall y \in \mathbf{R}$, $0 + y = y$.

42. $\exists \varepsilon > 0$ such that $\forall$ integer N, $\exists$ an integer n such that $n > N$ and either $L - \varepsilon \geq a_n$ or $a_n \geq L + \varepsilon$. In other words, there is a positive number ε such that for every integer N, it is possible to find an integer n that is greater than N and has the property that a_n does not lie between $L - \varepsilon$ and $L + \varepsilon$.

44. a. This statement is true. The unique real number with the given property is 1. Note that

$$1 \cdot y = y \text{ for all real numbers } y,$$

and if x is any real number such that for instance, $x \cdot 2 = 2$, then dividing both sides by 2 gives $x = 2/2 = 1$.

46. a. True. Both triangles a and c lie above all the squares.

b. *Formal version:*

$$\exists x(\text{Triangle}(x) \wedge (\forall y(\text{Square}(y) \rightarrow \text{Above}(x, y))))$$

c. *Formal negation:*

$$\forall x(\sim(\text{Triangle}(x) \wedge (\forall y(\text{Square}(y) \rightarrow \text{Above}(x, y)))))$$

$$\equiv \forall x(\sim\text{Triangle}(x) \vee \sim(\forall y\ (\text{Square}(y) \rightarrow \text{Above}(x, y))))$$

$$\equiv \forall x(\sim\text{Triangle}(x) \vee (\exists y\ (\text{Square}(y) \wedge \sim\text{Above}(x, y))))$$

48. a. False. There is no square to the right of circle k.

b. *Formal version:*

$$\forall x(\text{Circle}(x) \rightarrow (\exists y(\text{Square}(y) \wedge \text{RightOf}(y, x))))$$

c. *Formal negation:*

$$\exists x(\text{Circle}(x) \wedge \sim(\exists y(\text{Square}(y) \wedge \text{RightOf}(y, x))))$$

$$\equiv \exists x(\text{Circle}(x) \wedge \forall y(\sim\text{Square}(y) \vee \sim\text{RightOf}(y, x)))$$

49. a. False. For example circle d is gray and there is no square that is colored gray.

b. *Formal version:*

$$\forall x(\text{Circle}(x) \rightarrow \exists y(\text{Square}(y) \wedge \text{SameColor}(y, x)))$$

c. *Formal negation:*

$$\exists x(\sim(\text{Circle}(x) \rightarrow \exists y(\text{Square}(y) \wedge \text{SameColor}(y, x))))$$

$$\equiv \exists x(\text{Circle}(x) \wedge \sim(\exists y(\text{Square}(y) \wedge \text{SameColor}(y, x))))$$

$$\equiv \exists x(\text{Circle}(x) \wedge \forall y(\sim(\text{Square}(y) \wedge \text{SameColor}(y, x))))$$

$$\equiv \exists x(\text{Circle}(x) \wedge \forall y(\sim\text{Square}(y)) \vee \sim(\text{SameColor}(y, x)))$$

51. a. True. Square e has the property that every triangle above it has the same color e because e is colored blue and the only triangles above e, namely a and c, are also colored blue.

b. *Formal version:*

$$\exists x(\text{Square}(x) \wedge (\forall y(\text{Triangle}\ (y) \wedge \text{Above}(y, x)) \rightarrow \text{SameColor}(y, x)))$$

c. *Formal negation:*

$$\forall x(\sim(\text{Square}(x) \wedge (\forall y((\text{Triangle}(y) \wedge \text{Above}(y, x)) \rightarrow \text{SameColor}(y, x)))))$$

$$\equiv \forall x(\sim\text{Square}(x) \vee (\sim(\forall y((\text{Triangle}(y) \wedge \text{Above}(y, x)) \rightarrow \text{SameColor}(y, x)))))$$

$$\equiv \forall x(\sim\text{Square}(x) \vee \exists y(\sim((\text{Triangle}(y) \wedge \text{Above}(y, x)) \rightarrow \text{SameColor}(y, x))))$$

$$\equiv \forall x(\sim\text{Square}(x) \vee \exists y((\text{Triangle}(y) \wedge \text{Above}(y, x)) \wedge (\sim\text{SameColor}(y, x))))$$

53. a. True. Circle b and squares h and j are all colored black.

b. *Formal version:*

$$\exists x(\text{Circle}(x) \wedge \exists y(\text{Square}(y) \wedge \text{SameColor}(x, y)))$$

c. *Formal negation:*

$$\forall x(\sim \text{Circle}(x) \wedge \exists y(\text{Square}(y) \wedge \text{SameColor}(y, x)))$$

$$\equiv \forall x(\sim \text{Circle}(x) \vee \sim(\exists y(\text{Square}(y) \wedge \text{SameColor}(y, x))))$$

$$\equiv \forall x(\sim \text{Circle}(x) \vee \forall y(\sim \text{Square}(y) \vee \sim \text{SameColor}(y, x)))$$

55. a. No matter what the domain D or the predicates $P(x)$ and $Q(x)$ are, the given statements have the same truth value. If the statement "$\forall x$ in D, $(P(x) \wedge Q(x))$" is true, then $P(x) \wedge Q(x)$ is true for every x in D, which implies that both $P(x)$ and $Q(x)$ are true for every x in D. But then $P(x)$ is true for every x in D, and also $Q(x)$ is true for every x in D. So the statement "$(\forall x$ in D, $P(x)) \wedge (\forall x$, in D, $Q(x))$" is true. Conversely, if the statement "$(\forall x$ in D, $P(x)) \wedge (\forall x$ in D, $Q(x))$" is true, then $P(x)$ is true for every x in D, and also $Q(x)$ is true for every x in D. This implies that both $P(x)$ and $Q(x)$ are true for every x in D, and so $P(x) \wedge Q(x)$ is true for every x in D. Hence the statement "$\forall x$ in D, $(P(x) \wedge Q(x))$" is true.

59. a. Yes **b.** $X = w_1, X = w_2$ **c.** $X = b_2, X = w_2$

SECTION 3.4

1. b. $(f_i + f_j)^2 = f_i^2 + 2f_i f_j + f_j^2$

c. $(3u + 5v)^2 = (3u)^2 + 2(3u)(5v) + (5v)^2$

d. $(g(r) + g(s))^2 = (g(r))^2 + 2g(r)g(s) + (g(s))^2$

2. 0 is even.

3. $\frac{2}{3} + \frac{4}{5} = \frac{(2 \cdot 5 + 3 \cdot 4)}{(3 \cdot 5)} \left(= \frac{22}{15}\right)$

5. $\frac{1}{0}$ is not an irrational number.

7. Invalid; converse error

8. Valid by universal modus ponens (or universal instantiation)

9. Invalid; inverse error

10. Valid by universal modus tollens

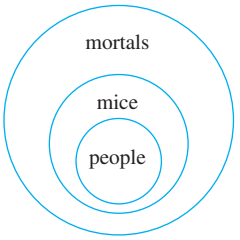
16. Invalid; converse error

19. $\forall x$, if x is a good car, then x is not cheap.

a. Valid, universal modus ponens (or universal instantiation)

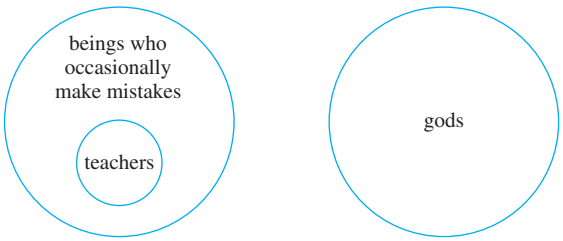
b. Invalid, converse error

21. Valid. (A valid argument can have false premises and a true conclusion!)



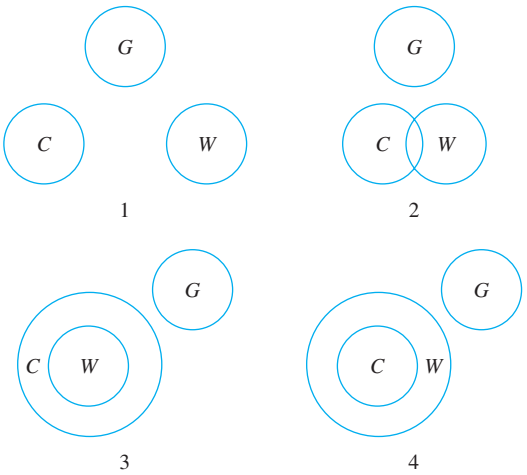
The major premise says the set of people is included in the set of mice. The minor premise says the set of mice is included in the set of mortals. Assuming both of these premises are true, it must follow that the set of people is included in the set of mortals. Since it is impossible for the conclusion to be false if the premises are true, the argument is valid.

23. Valid. The major and minor premises can be diagrammed as follows:



According to the diagram, the set of teachers and the set of gods can have no common elements. Hence, if the premises are true, then the conclusion must also be true, and so the argument is valid.

25. Invalid. Let C represent the set of all college cafeteria food, G the set of all good food, and W the set of all wasted food. Then any one of the following diagrams could represent the given premises.



Only in drawing (1) is the conclusion true. Hence it is possible for the premises to be true while the conclusion is false, and so the argument is invalid.

28. (3) *Contrapositive form:* If an object is gray, then it is a circle.

(2) If an object is a circle, then it is to the right of all the blue objects.

(1) If an object is to the right of all the blue objects, then it is above all the triangles.

$\therefore$ If an object is gray, then it is above all the triangles.

31. 4. If an animal is in the yard, then it is mine.

1. If an animal belongs to me, then I trust it.

5. If I trust an animal, then I admit it into my study.

3. If I admit an animal into my study, then it will beg when told to do so.

6. If an animal begs when told to do so, then that animal is a dog.

2. If an animal is a dog, then that animal gnaws bones.

$\therefore$ If an animal is in the yard, then that animal gnaws bones; that is, all the animals in the yard gnaw bones.

33. 2. If a bird is in this aviary, then it belongs to me.

4. If a bird belongs to me, then it is at least 9 feet high.

1. If a bird is at least 9 feet high, then it is an ostrich.

3. If a bird lives on mince pies, then it is not an ostrich.

Contrapositive: If a bird is an ostrich, then it does not live on mince pies.

$\therefore$ If a bird is in this aviary, then it does not live on mince pies; that is, no bird in this aviary lives on mince pies.

SECTION 4.1

1. a. Yes: $-17 = 2(-9) + 1$

b. No. 0 is even because $0 = 0 \cdot 2$.

c. Yes: $2k - 1 = 2(k - 1) + 1$ and $k - 1$ is an integer because it is a difference of integers.

3. a. Yes: $6m + 8n = 2(3m + 4n)$ and $(3m + 4n)$ is an integer because 3, 4, m, and n are integers, and products and sums of integers are integers.

b. Yes: $10mn + 7 = 2(5mn + 3) + 1$ and $5mn + 3$ is an integer because 3, 5, m, and n are integers, and products and sums of integers are integers.

c. Not necessarily. For instance, if $m = 3$ and $n = 2$, then $m^2 - n^2 = 9 - 4 = 5$, which is prime. (However, $m^2 - n^2$ is composite for many values of m and n because of the identity $m^2 - n^2 = (m - n)(m + n)$.)

5. For example, let $m = n = 2$. Then m and n are integers such that $m > 1$ and $n > 1$ and $\frac{1}{m} + \frac{1}{n} = \frac{1}{2} + \frac{1}{2} = 1$, which is an integer.

8. For example, let $n = 7$. Then n is an integer such that $n > 5$ and $2^n - 1 = 127$, which is prime.

10. For example, 25, 9, and 16 are all perfect squares, because $25 = 5^2$, $9 = 3^2$, and $16 = 4^2$, and $25 = 9 + 16$. Thus 25 is a perfect square that can be written as a sum of two other perfect squares.

12. a. *Negation for the statement:* There exist real numbers a and b such that $a < b$ and $a^2 \not< b^2$.

b. *Counterexample for the statement:* Let $a = -2$ and $b = -1$. Then $a < b$ because $-2 < -1$, but $a^2 \not< b^2$ because $(-2)^2 = 4$ and $(-1)^2 = 1$ and $4 \not< 1$. *[So the hypothesis of the statement is true and its conclusion is false.]*

14. Counterexample: Let $m = 2$ and $n = 1$. Then

$$2m + n = 2 \cdot 2 + 1 = 5,$$

which is odd. But m is not odd, and so it is false that both m and n are odd. *[This is one counterexample among many.]*

17. This property is true for some integers and false for other integers. For instance, if $a = 0$ and $b = 1$, the property is true because $(0 + 1)^2 = 0^2 + 1^2$, but if $a = 1$ and $b = 1$, the property is false because $(1 + 1)^2 = 4$ and $1^2 + 1^2 = 2$ and $4 \neq 2$.

19. *Hint:* This property is true for some integers and false for other integers. To justify this answer you need to find examples of both.

21. $2 = 1^2 + 1^2$, $4 = 2^2$, $6 = 2^2 + 1^2 + 1^2$,
$8 = 2^2 + 2^2$, $10 = 3^2 + 1^2$, $12 = 2^2 + 2^2 + 2^2$,
$14 = 3^2 + 2^2 + 1^2$, $16 = 4^2$,
$18 = 3^2 + 3^2 = 4^2 + 1^2 + 1^2$, $20 = 4^2 + 2^2$,
$22 = 3^2 + 3^2 + 2^2$, $24 = 4^2 + 2^2 + 2^2$

23. a. If an integer is greater than 1, then its reciprocal is between 0 and 1.

b. *Start of proof:* Suppose m is any integer such that $m > 1$. *Conclusion to be shown:* $0 < 1/m < 1$.

25. a. If the product of two integers is 1, then either both are 1 or both are -1.

b. *Start of proof:* Suppose m and n are any integers with $mn = 1$. *Conclusion to be shown:* $m = n = 1$ *or* $m = n = -1$.

27. *Hint:* (b) $2k + 1$

28. a. $\forall$ integers m and n, if m and n are odd then $m+n$ is odd.

$\forall$ odd integers m and n, $m+n$ is odd.

If m and n are any odd integers, then $m+n$ is odd.

b. (a) definition of odd, (b) substitution, (c) any sum of integers is an integer, (d) definition of even

30. a. $\forall$ integers m and n, if m is even and n is odd, then $m+n$ is odd.

$\forall$ even integers m and odd integers n, $m+n$ is odd.

If m is any even integer and n is any odd integer, then $m+n$ is odd.

b. (a) any odd integer

(b) integer r

(c) $2r+(2s+1)$

(d) $m+n$ is odd

SECTION 4.2

1. Proof: Suppose n is any *[particular but arbitrarily chosen]* odd integer.

[We must show that $3n+5$ is even. By definition of even, this means we must show that $3n+5 = 2\cdot$(some integer).]

By definition of odd, $n = 2r+1$ for some integer r.

Then

$$\begin{aligned} 3n+5 &= 3(2r+1)+5 && \text{by substitution} \\ &= 6r+3+5 \\ &= 6r+8 \\ &= 2(3r+4) && \text{by algebra.} \end{aligned}$$

[Idea for the rest of the proof: We want to show that $3n+5 = 2\cdot$(some integer). At this point we know that $3n+5 = 2(3r+4)$. So is $3r+4$ an integer? Yes, because products and sums of integers are integers.]

Let $k = 3r+4$.

Then $3n+5 = 2(3r+4) = 2k$, and k is an integer because products and sums of integers are integers. Hence $3n+5$ is even by definition of even.

3. *Hint:* To show that an integer is odd, you need to show that it equals $2\cdot$(some integer) $+1$.

4. *Two versions of a correct proof are given below to illustrate some of the variety that is possible.*

Proof 1: Suppose a is any even integer and b is any odd integer. *[We must show that $a-b$ is odd.]* By definition of even and odd, $a = 2r$ and $b = 2s+1$ for some integers r and s. By substitution and algebra,

$$a-b = 2r-(2s+1) = 2r-2s-1 = 2(r-s-1)+1.$$

Let $t = r-s-1$. Then t is an integer because differences of integers are integers. Thus $a-b = 2t+1$, where t is an integer, and so, by definition of odd, $a-b$ is odd *[as was to be shown]*.

Proof 2: Suppose a is any even integer and b is any odd integer. By definition of even and odd, $a = 2r$ and $b = 2s+1$ for some integers r and s. Then

$$a-b = 2r-(2s+1) = 2(r-s-1)+1.$$

Now $r-s-1$ is an integer because differences of integers are integers, and so $a-b$ equals twice some integer plus 1. Thus $a-b$ is odd.

6. Proof: Suppose k is any odd integer and m is any even integer. *[We must show that k^2+m^2 is odd.]* By definition of odd and even, $k = 2a+1$ and $m = 2b$ for some integers a and b. Then

$$\begin{aligned} k^2+m^2 &= (2a+1)^2+(2b)^2 && \text{by substitution} \\ &= 4a^2+4a+1+4b^2 \\ &= 4(a^2+a+b^2)+1 \\ &= 2(2a^2+2a+2b^2)+1 && \text{by algebra.} \end{aligned}$$

But $2a^2+2a+2b^2$ is an integer because it is a sum of products of integers. Thus k^2+m^2 is twice an integer plus 1, and so k^2+m^2 is odd *[as was to be shown]*.

7. *Hint:* It is convenient to represent two consecutive integers as n and $n+1$ or as $n-1$ and n for some integer n.

10. Proof: Suppose n is any even integer. Then $n = 2k$ for some integer k. Hence

$$(-1)^n = (-1)^{2k} = ((-1)^2)^k = 1^k = 1$$

[by the laws of exponents from algebra]. This is what was to be shown.

12. To prove the given statement is false, we prove that its negation is true.

The negation of the statement is "For every integer $m \geq 3$, m^2-1 is not prime."

Proof of the negation: Suppose m is any integer with $m \geq 3$. By basic algebra, $m^2-1 = (m-1)(m+1)$. Because $m \geq 3$, both $m-1$ and $m+1$ are positive integers greater than 1, and each is smaller than m^2-1. So m^2-1 is a product of two smaller positive integers, each greater than 1, and hence m^2-1 is not prime.

15. The incorrect proof just shows the theorem to be true in the one case where $k = 2$. A real proof must show that it is true for *every* integer $k > 0$.

16. The mistake in the "proof" is that the same symbol, k, is used to represent two different quantities. By setting $m = 2k$ and $n = 2k+1$, the proof implies that

$n = m + 1$, and thus it deduces the conclusion only for this one situation. When $m = 4$ and $n = 17$, for instance, the computations in the proof indicate that $n - m = 1$, but actually $n - m = 13$. In other words, the proof does not deduce the conclusion for an arbitrarily chosen even integer m and odd integer n, and hence it is invalid.

17. This incorrect proof assumes what is to be proved. The word *since* in the third sentence is completely unjustified. The second sentence tells only what happens *if* $k^2 + 2k + 1$ is composite. But at that point in the proof, it has not been established that $k^2 + 2k + 1$ *is* composite. In fact, that is exactly what is to be proved.

20. True. Proof: Suppose m and n are any odd integers. *[We must show that mn is odd.]* By definition of odd, $n = 2r + 1$ and $m = 2s + 1$ for some integers r and s. Then

$$\begin{aligned} mn &= (2r+1)(2s+1) && \text{by substitution} \\ &= 4rs + 2r + 2s + 1 \\ &= 2(2rs + r + s) + 1 && \text{by algebra.} \end{aligned}$$

Now $2rs + r + s$ is an integer because products and sums of integers are integers and 2, r, and s are all integers. Hence $mn = 2 \cdot$(some integer) $+ 1$, and so, by definition of odd, mn is odd.

21. *Hint:* You will need to express an integer of the form $-(2k + 1)$ as 2(*some integer*) $+ 1$.

22. False. Counterexample: Let $a = 1$ and $b = 0$. Then $4a + 5b + 3 = 4 \cdot 1 + 5 \cdot 0 + 3 = 7$, which is odd. *[This is one counterexample among many. Can you find a way to characterize all counterexamples?]*

24. False. Counterexample: Let $m = 1$ and $n = 3$. Then $m + n = 4$ is even, but neither summand m nor summand n is even.

28. *Hint:* The statement is true.

32. Proof: Suppose n is any integer. Then

$$\begin{aligned} 4(n^2 + n + 1) - 3n^2 &= 4n^2 + 4n + 4 - 3n^2 \\ &= n^2 + 4n + 4 = (n+2)^2 \end{aligned}$$

(by algebra). Now $(n + 2)^2$ is a perfect square because $n + 2$ is an integer (being a sum of n and 2). Hence $4(n^2 + n + 1) - 3n^2$ is a perfect square, as was to be shown.

34. *Hint:* This is true.

37. *Hint:* The statement is true.

40. *Hint:* The answer is no.

SECTION 4.3

1. $\frac{-35}{6} = \frac{-35}{6}$

3. $\frac{4}{5} + \frac{2}{9} = \frac{4 \cdot 9 + 2 \cdot 5}{45} = \frac{46}{45}$

4. Let $x = 0.3737373737\ldots$.

Then $100x = 37.37373737\ldots$, and so

$100x - x = 37.37373737\ldots - 0.3737373737\ldots$

Thus $99x = 37$, and hence $x = \frac{37}{99}$.

6. Let $x = 320.5492492492\ldots$. Then

$10000x = 3205492.492492492\ldots$, and

$10x = 3205.492492492\ldots$, and so

$10000x - 10x = 3205492 - 3205$.

Thus $9990x = 3202287$, and hence $x = \frac{3202287}{9990}$.

8. b. $\forall$ real numbers x and y, if $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.

9. Given that a and b are integers, both $b - a$ and ab^2 are integers (since differences and products of integers are integers). Also, by the zero product property, $ab^2 \neq 0$ because neither a nor b is zero. Hence $(b - a)/ab^2$ is a quotient of two integers with a nonzero denominator, and so it is rational.

11. Proof: Suppose n is any *[particular but arbitrarily chosen]* integer. Then $n = n \cdot 1$, and so $n = n/1$ by dividing both sides by 1. Now n and 1 are both integers, and $1 \neq 0$. Hence n can be written as a quotient of integers with a nonzero denominator, and so n is rational.

12. **(a)** any *[particular but arbitrarily chosen]* rational number
(b) integers a and b
(c) $(a/b)^2$
(d) b^2
(e) zero product property
(f) r^2 is rational

13. a. $\forall$ real number r, if r is rational then $-r$ is rational.

Or: $\forall r$, if r is a rational number then $-r$ is rational.

Or: $\forall$ rational number r, $-r$ is rational.

b. The statement is true. Proof: Suppose r is a *[particular but arbitrarily chosen]* rational number. *[We must show that $-r$ is rational.]* By definition of rational, $r = a/b$ for some integers a and b with $b \neq 0$. Then

$$\begin{aligned} -r &= -\frac{a}{b} && \text{by substitution} \\ &= \frac{-a}{b} && \text{by algebra.} \end{aligned}$$

Now since a is an integer, so is $-a$ (being the product of -1 and a). Hence $-r$ is a quotient of integers with a nonzero denominator, and so $-r$ is rational *[as was to be shown]*.

15. Proof: Suppose r and s are rational numbers. By definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Then

$$rs = \frac{a}{b}\cdot\frac{c}{d} \quad \text{by substitution}$$
$$= \frac{ac}{bd} \quad \text{by the rules of algebra for multiplying fractions.}$$

Now ac and bd are both integers (being products of integers) and $bd \neq 0$ (by the zero product property). Hence rs is a quotient of integers with a nonzero denominator, and so, by definition of rational, rs is rational.

16. *Hint:* Counterexample: Let r be any rational number and $s = 0$. Then r and s are both rational, but the quotient of r divided by s is not a real number and therefore is not a rational number.

Revised statement to be proved: For all rational numbers r and s, if $s \neq 0$ then r/s is rational.

17. *Hint:* The conclusion to be shown is that a certain quantity (the difference of two rational numbers) is rational. To show this, you need to show that the quantity can be expressed as a ratio of two integers with a nonzero denominator.

18. *Hint:* $\dfrac{a/b + c/d}{2} = \dfrac{(ad+bc)/(bd)}{2} = \dfrac{ad+bc}{2bd}$.

19. *Hint:* If $a < b$ then $a + a < a + b$ (by T19 of Appendix A), or equivalently, $2a < a + b$. Thus $a < \frac{a+b}{2}$ (by T20 of Appendix A).

21. True. Proof: Suppose m is any even integer and n is any odd integer. *[We must show that $m^2 + 3n$ is odd.]* By properties 1 and 3 of Example 4.3.3, m is even (because $m^2 = m \cdot m$) and $3n$ is odd (because both 3 and n are odd). It follows from property 5 *[and the commutative law for addition]* that $m^2 + 3n$ is odd *[as was to be shown]*.

24. Proof: Suppose r and s are any rational numbers. By Theorem 4.3.1, both 2 and 3 are rational, and so, by exercise 15, both $2r$ and $3s$ are rational. Hence, by Theorem 4.3.2, $2r + 3s$ is rational.

27. Let

$$x = \frac{1-\dfrac{1}{2^{n+1}}}{1-\dfrac{1}{2}} = \frac{1-\dfrac{1}{2^{n+1}}}{\dfrac{1}{2}} = \frac{1-\dfrac{1}{2^{n+1}}}{\dfrac{1}{2}}\cdot\frac{2^{n+1}}{2^{n+1}} = \frac{2^{n+1}-1}{2^n}.$$

Now $2^{n+1} - 1$ and 2^n are both integers (since n is a nonnegative integer) and $2^n \neq 0$ by the zero product property. Therefore, x is rational.

31. Proof: Suppose c is a real number such that

$$r_3c^3 + r_2c^2 + r_1c + r_0 = 0,$$

where r_0, r_1, r_2, and r_3 are rational numbers. By definition of rational, $r_0 = a_0/b_0$, $r_1 = a_1/b_1$, $r_2 = a_2/b_2$, and $r_3 = a_3/b_3$ for some integers, a_0, a_1, a_2, a_3, and nonzero integers b_0, b_1, b_2, and b_3. By substitution,

$$\begin{aligned} &r_3c^3 + r_2c^2 + r_1c + r_0 \\ &\quad = \frac{a_3}{b_3}c_3 + \frac{a_2}{b_2}c_2 + \frac{a_1}{b_1}c_1 + \frac{a_0}{b_0} \\ &\quad = \frac{b_0b_1b_2a_3}{b_0b_1b_2b_3}c^3 + \frac{b_0b_1b_3a_2}{b_0b_1b_2b_3}c^2 + \frac{b_0b_2b_3a_1}{b_0b_1b_2b_3}c + \frac{b_1b_2b_3a_0}{b_0b_1b_2b_3} \\ &\quad = 0. \end{aligned}$$

Multiplying both sides by $b_0b_1b_2b_3$ gives

$$b_0b_1b_2a_3 \cdot c^3 + b_0b_1b_3a_2 \cdot c^2 + b_0b_2b_3a_1 \cdot c + b_1b_2b_3a_0 = 0.$$

Let $n_3 = b_0b_1b_2a_3$, $n_2 = b_0b_1b_3a_2$, $n_1 = b_0b_2b_3a_1$, and $n_0 = b_1b_2b_3a_0$. Then n_0, n_1, n_2, and n_3 are all integers (being products of integers). Hence c satisfies the equation

$$n_3c^3 + n_2c^2 + n_1c + n_0 = 0,$$

where all of n_0, n_1, n_2, and n_3 are integers. This is what was to be shown.

33. a. *Hint:* Note that $(x - r)(x - s) = x^2 - (r + s)x + rs$. If both r and s are odd, then $r + s$ is even and rs is odd. So the coefficient of x^2 is 1 (odd), the coefficient of x is even, and the constant coefficient, rs, is odd.

35. This "proof" assumes what is to be proved.

37. By setting both r and s equal to a/b, this incorrect proof violates the requirement that r and s be arbitrarily chosen rational numbers. If both r and s equal a/b, then $r = s$.

SECTION 4.4

1. Yes, $52 = 13 \cdot 4$

2. Yes, $56 = 7 \cdot 8$

4. Yes, $(3k + 1)(3k + 2)(3k + 3) = 3[(3k + 1)(3k + 2)(k + 1)]$, and $(3k + 1)(3k + 2)(k + 1)$ is an integer because k is an integer and sums and products of integers are integers.

6. No, $29/3 \cong 9.67$, which is not an integer.

7. Yes, $66 = (-3)(-22)$.

8. Yes, $6a(a+b) = 3a[2(a+b)]$, and $2(a+b)$ is an integer because a and b are integers and sums and products of integers are integers.

10. No, $34/7 \cong 4.86$, which is not an integer.

12. Yes, $n^2 - 1 = (4k+1)^2 - 1 = (16k^2 + 8k + 1) - 1 = 16k^2 + 8k = 8(2k^2 + k)$, and $2k^2 + k$ is an integer because k is an integer and sums and products of integers are integers.

14. **(a)** $a \mid b$
(b) $b = a \cdot r$
(c) $-r$
(d) $a \mid (-b)$

15. Proof: Suppose a, b, and c are any integers such that $a \mid b$ and $a \mid c$. *[We must show that $a \mid (b+c)$.]* By definition of divides, $b = ar$ and $c = as$ for some integers r and s. Then

$$b + c = ar + as = a(r+s) \qquad \text{by algebra.}$$

Let $t = r + s$. Then t is an integer (being a sum of integers), and thus $b + c = at$ where t is an integer. By definition of divides, then, $a \mid (b+c)$ *[as was to be shown].*

16. *Hint:* The conclusion to be shown is that a certain quantity is divisible by a. To show this, you need to show that the quantity equals a times some integer.

18. **a.** $\forall$ integers n if n is a multiple of 3 then $-n$ is a multiple of 3.
b. The statement is true. Proof: Suppose n is any integer that is a multiple of 3. *[We must show that $-n$ is a multiple of 3.]* By definition of multiple, $n = 3k$ for some integer k. Then

$$-n = -(3k) \qquad \text{by substitution}$$
$$= 3(-k) \qquad \text{by algebra.}$$

Now $-k$ is an integer because k is. Hence, by definition of multiple, $-n$ is a multiple of 3 *[as was to be shown].*

19. Counterexample: Let $a = 2$ and $b = 1$. Then $a + b = 2 + 1 = 3$, and so $3 \mid (a+b)$ because $3 = 3 \cdot 1$. On the other hand, $a - b = 2 - 1 = 1$, and $3 \nmid 1$ because $1/3$ is not an integer. Thus $3 \nmid (a-b)$. *[So the hypothesis of the statement is true and its conclusion is false.]*

20. *Hint:* The consecutive integers can be conveniently represented as $n-1$, n, and $n+1$ or as n, $n+1$, $n+2$, where n is an integer.

22. *Hint:* The given statement can be rewritten formally as "$\forall$ integers n, if n is divisible by 6 then n is divisible by 2." This statement is true.

24. The statement is true. Proof: Suppose a, b, and c are any integers such that $a \mid b$ and $a \mid c$. *[We must show that $a \mid (2b - 3c)$.]* By definition of divisibility, we know that $b = am$ and $c = an$ for some integers m and n. It follows that $2b - 3c = 2(am) - 3(an)$ *(by substitution)* $= a(2m - 3n)$ *(by basic algebra)*. Let $t = 2m - 3n$. Then t is an integer because it is a difference of products of integers. Hence $2b - 3c = at$, where t is an integer, and so $a \mid (2b - 3c)$ by definition of divisibility *[as was to be shown].*

25. The statement is false. Counterexample: Let $a = 2$, $b = 8$, and $c = 8$. Then a is a factor of c because $8 = 2 \cdot 4$ and b is a factor of c because $8 = 1 \cdot 8$, but $ab = 16$ and 16 is not a factor of 8 because $8 \neq 16 \cdot k$ for any integer k since $8/16 = 1/2$.

26. *Hint:* The statement is true.

27. *Hint:* The statement is false.

32. No. Each of these numbers is divisible by 3, and so their sum is also divisible by 3. But 100 is not divisible by 3. Thus the sum cannot equal \$100.

36. **a.** The sum of the digits is 54, which is divisible by 9. Therefore, 637,425,403,705,125 is divisible by 9 and hence also divisible by 3 (by transitivity of divisibility). Because the rightmost digit is 5, then 637,425,403,705,125 is divisible by 5. And because the two rightmost digits are 25, which is not divisible by 4, then 637,425,403,705,125 is not divisible by 4.

37. **a.** $1{,}176 = 2^3 \cdot 3 \cdot 7^2$

38. **a.** $8{,}424 = 2^3 \cdot 3^4 \cdot 13$
c. *Hint:* The answer is no. Note that each factor of 10 is comprised of a factor of 2 and a factor of 5.
d. *Hint:* The answer is 26. Note that in order for $8{,}424 \cdot m$ to be a perfect square, each prime factor must be raised to an even power.

40. **a.** Because $12a = 25b$, the unique factorization theorem guarantees that the standard factored forms of $12a$ and $25b$ must be the same. Thus $25b$ contains the factors $2^2 \cdot 3$ $(=12)$. But since neither 2 nor 3 divides 25, the factors $2^2 \cdot 3$ must all occur in b, and hence $12 \mid b$. Similarly, $12a$ contains the factors $5^2 = 25$, and since 5 is not a factor of 12, the factors 5^2 must occur in a. So $25 \mid a$.

41. *Hint:* $45^8 \cdot 88^5 = (3^2 \cdot 5)^8 \cdot (2^3 \cdot 11)^5 = 3^{16} \cdot 5^8 \cdot 2^{15} \cdot 11^5$. How many factors of 10 does this number contain?

42. **a.** $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2 = 2^4 \cdot 3^2 \cdot 5$

43. *Hint:* There are 108 mathematics students and 120 computer science students at the university.

44. Proof: Suppose n is a nonnegative integer whose decimal representation ends in 0. Then $n = 10m + 0 = 10m$ for some integer m. Factoring out a 5 yields $n = 10m = 5(2m)$, and $2m$ is an integer since m is an integer. Hence $10m$ is divisible by 5, which is what was to be shown.

47. *Hint:* You may take it as a fact that for any positive integer k,

$$10^k = \underbrace{99\ \ldots\ 9}_{k \text{ of these}} + 1; \quad \text{that is,}$$

$$10^k = 9\cdot 10^{k-1} + 9\cdot 10^{k-2} + \cdots + 9\cdot 10^1 + 9\cdot 10^0 + 1.$$

SECTION 4.5

1. $q = 7, r = 7$ **3.** $q = 0, r = 36$

5. $q = -5, r = 10$

7. **a.** 4 **b.** 7

11. **a.** When today is Saturday, 15 days from today is two weeks (which is Saturday) plus one day (which is Sunday). Hence *DayN* should be 0. According to the formula, when today is Saturday, $DayT = 6$, and so when $N = 15$,

$$\begin{aligned} DayN &= (DayT + N) \ mod\ 7 \\ &= (6 + 15) \ mod\ 7 \\ &= 21 \ mod\ 7 = 0, \text{ which agrees.} \end{aligned}$$

13. *Solution 1:* $30 = 4\cdot 7 + 2$. Hence the answer is two days after Monday, which is Wednesday.

Solution 2: By the formula, the answer is $(1 + 30) \ mod\ 7 = 31 \ mod\ 7 = 3$, which is Wednesday.

14. *Hint:* There are two ways to solve this problem. One is to find that $1{,}000 = 7\cdot 142 + 6$ and note that if today is Tuesday, then 1,000 days from today is 142 weeks plus 6 days from today. The other way is to use the formula $DayN = (DayT + N) \ mod\ 7$, with $DayT = 2$ (Tuesday) and $N = 1{,}000$.

16. Because $d|n$, $n = dq + 0$ for some integer q. Thus the remainder is 0.

18. Proof: Suppose n is any odd integer. By definition of odd, $n = 2q + 1$ for some integer q. Then $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 = 4q(q + 1) + 1$. By the result of part (a), the product $q(q + 1)$ is even, so $q(q + 1) = 2m$ for some integer m. Then, by substitution, $n^2 = 4\cdot 2m + 1 = 8m + 1$.

20. Because $a \ mod\ 7 = 4$, the remainder obtained when a is divided by 7 is 4, and so $a = 7q + 4$ for some integer q. Multiplying this equation through by 5 gives that $5a = 35q + 20 = 35q + 14 + 6 = 7(5q + 2) + 6$. Because q is an integer, $5q + 2$ is also an integer, and so $5a = 7\cdot(\text{an integer}) + 6$. Thus, because $0 \le 6 < 7$, the remainder obtained when $5a$ is divided by 7 is 6, and so $5a \ mod\ 7 = 6$.

23. Proof: Suppose n is any *[particular but arbitrarily chosen]* integer such that $n \ mod\ 5 = 3$. Then the remainder obtained when n is divided by 5 is 3, and so $n = 5q + 3$ for some integer q. By substitution,

$$\begin{aligned} n^2 &= (5q + 3)^2 = 25q^2 + 30q + 9 \\ &= 25q^2 + 30q + 5 + 4 = 5(5q^2 + 6q + 1) + 4. \end{aligned}$$

Because products and sums of integers are integers, $5q^2 + 6q + 1$ is an integer, and hence $n^2 = 5\cdot(\text{an integer}) + 4$.

Thus, since $0 \le 4 < 5$, the remainder obtained when n^2 is divided by 5 is 4, and so $n^2 \ mod\ 5 = 4$.

26. *Hint:* You need to show that (1) for each integer n and positive integer d, if n is divisible by d then $n \ mod\ d = 0$; and (2) for each integer n and positive integer d, if $n \ mod\ d = 0$ then n is divisible by d.

27. *Hint:* Given any integer n, by the quotient-remainder theorem with divisor equal to 2, $n = 2q$, or $n = 2q + 1$ for some integer q.

28. **a.** *Hint:* Start by supposing that n, $n + 1$, and $n + 2$ are any three consecutive integers. Then use the quotient-remainder theorem to divide into three cases:

***Case 1* ($n = 3q$ *for some integer* q).** In this case you will show that n is a multiple of 3.

***Case 2* ($n = 3q + 1$ *for some integer* q).** In this case you will show that $n + 2$ is a multiple of 3.

***Case 3* ($n = 3q + 2$ *for some integer* q).** In this case you will show that $n + 1$ is a multiple of 3.

Conclude that in all possible cases one of the integers is a multiple of 3.

29. **a.** *Hint:* Given any integer n, begin by using the quotient-remainder theorem to say that n can be written in one of the three forms: $n = 3q$, or $n = 3q + 1$, or $n = 3q + 2$ for some integer q. Then divide into three cases according to these three possibilities. Show that in each case either $n^2 = 3k$ for some integer k, or $n^2 = 3k + 1$ for some integer k. For instance, when $n = 3q + 2$, then $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$, and $3q^2 + 4q + 1$ is an integer because it is a sum of products of integers.

31. b. If $m^2 - n^2 = 56$, then $56 = (m+n)(m-n)$. Now $56 = 2^3 \cdot 7$, and by the unique factorization theorem, this factorization is unique. Hence the only representation of 56 as a product of two positive integers are $56 = 7 \cdot 8 = 14 \cdot 4 = 28 \cdot 2 = 56 \cdot 1$. By part (a), m and n must both be odd or both be even. Thus the only solutions are either $m + n = 14$ and $m - n = 4$ or $m + n = 28$ and $m - n = 2$. It follows that the only solutions are either $m = 9$ and $n = 5$ or $m = 15$ and $n = 13$.

32. Under the given conditions, $2a - (b + c)$ is even.
Proof: Suppose a, b, and c are any integers such that $a - b$ is even and $b - c$ is even. *[We must show that $2a - (b + c)$ is even.]* Note first that $2a - (b + c) = (a - b) + (a - c)$. Also note that $(a - b) + (b - c)$ is a sum of two even integers and hence is even by Example 4.3.3 #1. But $(a - b) + (b - c) = a - c$, and so $a - c$ is even. Hence $2a - (b + c)$ is a sum of two even integers, and thus it is even *[as was to be shown].*

34. *Hint:* Express n using the quotient-remainder theorem with $d = 3$.

36. *Hint:* Use the quotient-remainder theorem (as in Example 4.5.6) to say that $n = 4q$, $n = 4q + 1$, $n = 4q + 2$, or $n = 4q + 3$ and divide into cases accordingly.

37. *Hint:* Given any integer n, consider the two cases where n is even and where n is odd.

39. *Hint:* Use the quotient-remainder theorem to say that p must have one of the forms $6q$, $6q + 1$, $6q + 2$, $6q + 3$, $6q + 4$, or $6q + 5$ for some integer q. Then use the fact that p is prime and not equal to either 2 or 3 to show that you only need to consider two cases.

41. *Hint:* There are four cases: Either x and y are both positive, or x is positive and y is negative, or x is negative and y is positive, or both x and y are negative.

43. *Hint:* Apply the triangle inequality with $x = a - b$ and $y = b$ and with $x = b - a$ and $y = a$. Then use the result of exercise 42.

44. a. $7{,}609 + 5 = 7{,}614$

46. *Answer to first question:* No. Counterexample: Let $m = 1$, $n = 3$, and $d = 2$. Then $m \bmod d = 1$ and $n \bmod d = 1$ but $m \neq n$.

Answer to second question: Yes. Proof: Suppose m, n, and d are integers such that $m \bmod d = n \bmod d$. Let $r = m \bmod d = n \bmod d$. By definition of *mod*, $m = dp + r$ and $n = dq + r$ for some integers p and q. Then $m - n = (dp + r) - (dq + r) = d(p - q)$. But $p - q$ is an integer (being a difference of integers), and so $m - n$ is divisible by d by definition of divisible.

SECTION 4.6

1. $\lfloor 37.999 \rfloor = 37$, $\lceil 37.999 \rceil = 38$

3. $\lfloor -14.00001 \rfloor = -15$, $\lceil -14.00001 \rceil = -14$

8. $\lfloor n/7 \rfloor$. The floor notation is more appropriate. If the ceiling notation is used, two different formulas are needed, depending on whether $n/7$ is an integer or not. (What are they?)

10. a. (i) $\left(2050 + \left\lfloor \frac{2049}{4} \right\rfloor - \left\lfloor \frac{2049}{100} \right\rfloor + \left\lfloor \frac{2049}{400} \right\rfloor\right) \bmod 7$
$= (2050 + 512 - 20 + 5) \bmod 7 = 2547 \bmod 7$
$= 6$, which corresponds to a Saturday.

b. *Hint:* One day is added every four years, except that each century the day is not added unless the century is a multiple of 400.

12. *Hint:* The mistake is assuming what is to be proved. Explain the way in which the mistake occurs in the "proof."

13. Proof: Suppose n is any even integer. By definition of even, $n = 2k$ for some integer k. Then

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k \qquad \text{because } k \text{ is an integer and } k \leq k < k - 1.$$

But $$k = \frac{n}{2} \qquad \text{because } n = 2k.$$

Thus, on the one hand, $\left\lfloor \frac{n}{2} \right\rfloor = k$, and on the other hand, $k = \frac{n}{2}$. It follows that $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ *[as was to be shown].*

14. Counterexample: Let $x = 2$ and $y = 1.9$.
Then $\lfloor x - y \rfloor = \lfloor 2 - 1.9 \rfloor = \lfloor 0.1 \rfloor = 0$, whereas $\lfloor x \rfloor - \lfloor y \rfloor = \lfloor 2 \rfloor - \lfloor 1.9 \rfloor = 2 - 1 = 1$.

15. Proof: Suppose x is any real number. Let $m = \lfloor x \rfloor$. By definition of floor, $m \leq x < m + 1$. Subtracting 1 from all parts of the inequality gives that

$$m - 1 \leq x - 1 < m,$$

and so, by definition of floor, $\lfloor x - 1 \rfloor = m - 1$. It follows by substitution that $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$.

17. *Proof for the case where $n \bmod 3 = 2$:*

In the case where $n \bmod 3 = 2$, then $n = 3q + 2$ for some integer q by definition of *mod*. By substitution,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{3q + 2}{3} \right\rfloor$$
$$= \left\lfloor \frac{3q}{3} + \frac{2}{3} \right\rfloor$$
$$= \left\lfloor q + \frac{2}{3} \right\rfloor = q \qquad \text{because } q \text{ is an integer and } q \leq q + 2/3 < q + 1.$$

But

$$q = \frac{n-2}{3} \qquad \text{by solving } n = 3q+2 \text{ for } q.$$

Thus, on the one hand, $\left\lfloor \frac{n}{3} \right\rfloor = q$, and on the other hand, $q = \frac{n-2}{3}$. It follows that $\left\lfloor \frac{n}{3} \right\rfloor = \frac{n-2}{3}$.

18. *Hint:* This is false.

19. *Hint:* This is true.

23. Proof: Suppose x is a real number that is not an integer. Let $\lfloor x \rfloor = n$. Then, by definition of floor and because x is not an integer, $n < x < n+1$. Multiplying both sides by -1 gives $-n > -x > -n-1$, or equivalently, $-n-1 < -x < -n$. Since $-n-1$ is an integer, it follows by definition of floor that $\lfloor -x \rfloor = -n-1$. Hence

$$\lfloor x \rfloor + \lfloor -x \rfloor = n + (-n-1) = n - n - 1 = -1,$$

as was to be shown.

25. *Hint:* Let $n = \left\lfloor \frac{x}{2} \right\rfloor$ and consider the two cases: n is even and n is odd.

26. Proof: Suppose x is any real number such that $x - \lfloor x \rfloor < \frac{1}{2}$. Multiplying both sides by 2 gives

$$2x - 2\lfloor x \rfloor < 1, \text{ or } 2x < 2\lfloor x \rfloor + 1.$$

Now by definition of floor, $\lfloor x \rfloor \le x$. Hence, $2\lfloor x \rfloor \le 2x$. Putting the two inequalities involving $2x$ together gives

$$2\lfloor x \rfloor \le 2x < 2\lfloor x \rfloor + 1.$$

Thus, by definition of floor (and because $2\lfloor x \rfloor$ is an integer), $\lfloor 2x \rfloor = 2\lfloor x \rfloor$. This is what to be shown.

28. *Hint:* After applying the hypothesis that n is odd, evaluate the two sides of the equation separately and show that the results are equal.

30. *Hint:* Divided into two cases: n is even and n is odd. For each case evaluate the two sides of the equation separately and show that the results are equal.

31. *Hint:* Start by dividing the proof into two cases: n is even and n is odd. In case n is odd, use the quotient-remainder theorem with divisor equal to 6 to divide into three cases: $n = 6k+1$, $n = 6k+3$, and $n = 6k+5$ for some integer k. You will need to consider a total of four cases.

SECTION 4.7

1. **(a)** a contradiction
(b) a positive real number
(c) x
(d) both sides by 2
(e) contradiction

3. Proof: Suppose not. That is, suppose there is an integer n such that $3n+2$ is divisible by 3. *[We must show that this supposition leads to a contradiction.]* By definition of divisibility, $3n+2 = 3k$ for some integer k. Subtracting 2 from both sides gives that $3n = 3k+2$, and subtracting $3k$ from both sides gives $3n - 3k = 2$, which implies that $3(n-k) = 2$ by factoring out 3. Dividing both sides by 3 gives $n - k = 2/3$. Now $n-k$ is an integer (because it is a difference of integers) and $2/3$ is not an integer. Since an integer cannot equal a non-integer, we have reached a contradiction. *[Hence the supposition is false and the given statement is true.]*

5. *Negation for the statement:* There is a greatest even integer.

Proof of the statement: Suppose not. That is, suppose there is a greatest even integer; call it N. Then N is an even integer, and $N \ge n$ for every even integer n. *[We must deduce a contradiction.]* Let $M = N+2$. Then M is an even integer since it is a sum of even integers, and $M > N$ since $M = N+2$. This contradicts the supposition that $N \ge n$ for *every* even integer n. *[Hence the supposition is false and the statement is true.]*

8. **(a)** a rational number
(b) an irrational number
(c) $\frac{a}{b}$
(d) $\frac{c}{d}$
(e) $\frac{a}{b} - \frac{c}{d}$
(f) integers
(g) integers
(h) zero product property
(i) rational

9. **a.** The mistake in this proof occurs in the second sentence where the negation written by the student is incorrect: instead of being existential, it is universal. The problem is that if the student proceeds in a logically correct manner, all that is needed to reach a contradiction is one example of a rational and an irrational number whose difference is irrational. To prove the given statement, however, it is necessary to show that there is *no* rational number and *no* irrational number whose difference is rational.

10. The mistake is that the negation for S that was used in the "proof" is incorrect. Thus deducing a contradiction from it fails to prove that S is true. (The actual negation is "There exist positive real numbers r and s such that $\sqrt{r+s} = \sqrt{r} + \sqrt{s}$.")

12. **a.** *Negation for R:* There exists an irrational number whose square root is rational.
b. Proof of R by contradiction: Suppose not. That is, suppose there exists an irrational number x such that the square root of x is rational. *[We must derive a*

contradiction.] By definition of rational, $\sqrt{x} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. By substitution,

$$(\sqrt{x})^2 = \left(\frac{a}{b}\right)^2,$$

and so, by algebra,

$$x = \frac{a^2}{b^2}.$$

But a^2 and b^2 are both products of integers and thus are integers, and b^2 is nonzero by the zero product property. Thus $\frac{a^2}{b^2}$ is rational. It follows that x is both irrational and rational, which is a contradiction. *[This is what was to be shown.]*

13. a. *Negation for S:* There exist an irrational number and a nonzero rational number whose product is rational.

14. b. *Hint:* Recall that to say $a \textit{ mod } 6 = 3$ means that there exists an integer r such that $a = 6r + 3$.

15. *Hint:* You could argue directly from the definition of odd, or you could use a result from Example 4.3.2.

16. Proof by contradiction: Suppose not. That is, suppose that there exist odd integers a and b such that $b^2 - a^2 = 4$. *[We must show that this supposition leads logically to a contradiction.]* Factoring gives that

$$b^2 - a^2 = (b + a)(b - a) = 4.$$

Now $b > a$ because $b^2 - a^2 = 4 > 0$, and the only way to factor 4 is either $4 = 2 \cdot 2$ or $4 = 4 \cdot 1$. Hence either $b + a = b - a = 2$, or $b + a = 4$ and $b - a = 1$ or $b + a = 1$ and $b - a = 4$.

In case $b + a = b - a = 2$, then $-a = a$ and so $a = 0$, which is not an odd integer.

In case $b + a = 4$ and $b - a = 1$, then $2b = 5$ and so $b = 5/2$, which is not an odd integer.

In case $b + a = 1$ and $b - a = 4$, then $2b = 5$ and so $b = 5/2$, which is not an odd integer.

Thus there are no odd integers a and b such that $b^2 - a^2 = 4$, which contradicts the supposition. *[Hence the supposition is false and the given statement is true.]*

17. *Hint:* Use the fact that $a^2 = c^2 - b^2 = (c - b)(c + b)$ and apply the unique factorization of integers theorem.

19. *Hint:* Suppose $n^2 - 2$ is divisible by 4, and consider the two cases where n is even and n is odd. (An alternative solution uses Proposition 4.7.4.)

20. a. $5 | n$
b. $5 | n^2$
c. $5k$
d. $(5k)^2$
e. $5 | n^2$

21. a. Proof by contradiction: Suppose not. That is, suppose there is an integer n such that n^2 is odd and n is even. Show that this supposition leads logically to a contradiction.
b. Proof by contraposition: Suppose n is any integer such that n is not odd. Show that n^2 is not odd.

23. *Formal version of the statement to be proved:* For every real number x, if x is irrational then $-x$ is irrational.

Proof by contraposition: Suppose x is any real number such that $-x$ is not irrational. By definition of irrational this means that $-x$ is rational. *[We must show that x is not irrational, or, equivalently, that x is rational.]* By definition of rational, $-x = a/b$ for some integers a and b with $b \neq 0$. Then, by algebra,

$$x = -(-x) = -(a/b) = (-a)/b.$$

Now $-a$ is an integer because a is an integer and because $-a = (-1)a$. Also b is a nonzero integer. Thus x is a ratio of integers with a nonzero denominator, and hence x is rational *[as was to be shown].*

Proof by contradiction: Suppose there exists a real number x such that x is irrational and $-x$ is not irrational. *[We must show that this supposition leads logically to a contradiction.]* By definition of rational, $-x = a/b$ for some integers a and b with $b \neq 0$. Then, by algebra,

$$x = -(-x) = -(a/b) = (-a)/b.$$

Now $-a$ is an integer because a is an integer and because $-a = (-1)a$. Also b is a nonzero integer. Thus x is a ratio of integers with a nonzero denominator, and hence x is rational. Hence x is both irrational and rational, which is a contradiction *[which shows that the negation is false and therefore that the statement to be proved is true].*

25. *Hint:* See the answer to exercise 21 and look carefully at the two proofs for Proposition 4.7.4.

26. Proof by contraposition: Suppose a, b, and c are any *[particular but arbitrarily chosen]* integers such that $a | b$. *[We must show that $a | bc$.]* By definition of divides, $b = ak$ for some integer k. Then $bc = (ak)c = a(kc)$. But kc is an integer (because it is a product of the integers k and c). Hence $a | bc$ by definition of divisibility *[as was to be shown].*

Proof by contradiction: Suppose not. *[We take the negation and suppose it to be true.]* Suppose $\exists$ integers a, b, and c such that $a \nmid bc$ and $a | b$. Since $a | b$, there exists an integer k such that $b = ak$ by definition of divides. Then $bc = (ak)c = a(kc)$ *[by the associative law of algebra].* But kc is an integer (being a product of integers), and so $a | bc$ by definition of divides. Thus $a \nmid bc$ and $a | bc$, which is a contradiction. *[This contradiction shows that the supposition is false, and hence the given statement is true.]*

28. *Hint:* To prove $p \to q \vee r$, it suffices to prove either $p \wedge \sim q \to r$ or $p \wedge \sim r \to q$. See exercise 14 in Section 2.2.

29. *Hints:* (1) The contrapositive is "For all integers m and n, if m and n are not both even and m and n are not both odd, then $m + n$ is not even." *Equivalently:* "For all integers m and n, if one of m and n is even and the other is odd, then $m + n$ is odd."

(2) The negation of the given statement is the following: $\exists$ integers m and n such that $m + n$ is even, and either m is even and n is odd, or m is odd and n is even.

31. a. Proof by contraposition: Suppose n, r, and s are positive integers and $r > \sqrt{n}$ and $s > \sqrt{n}$. *[We must show that $rs > n$.]* By Theorem T27 in Appendix A (with $a = r$, $b = s$, and $c = d = \sqrt{n}$), $rs > \sqrt{n} \cdot \sqrt{n} = n$. Thus the contrapositive of the given statement is true, and so the given statement is also true.

32. a. $\sqrt{667} \cong 25.8$, and so the possible prime factors to be checked are 2, 3, 5, 7, 11, 13, 17, 19, and 23. Testing each in turn shows that 667 is not prime because $667 = 23 \cdot 29$.

b. $\sqrt{557} \cong 23.6$, and so the possible prime factors to be checked are 2, 3, 5, 7, 11, 13, 17, 19, and 23. Testing each in turn shows that none divides 557. Therefore, 557 is prime.

34. a. $\sqrt{9269} \cong 96.3$, and so the possible prime factors to be checked are all among those you found for exercise 33. Testing each in turn shows that 9,269 is not prime because $9{,}269 = 13 \cdot 713$.

b. $\sqrt{9103} \cong 95.4$, and so the possible prime factors to be checked are all among those you found for exercise 33. Testing each in turn shows that none divides 9,103. Therefore, 9,103 is prime.

35. *Hint:* Assuming that n is not composite, show that $n - 4$, $n - 6$, and $n - 8$ are all prime. Next show that $n - 7$ is divisible by 3 by considering $n - 6$, $n - 7$, and $n - 8$. Finally, write $n - 4 = (n - 7) + 3$ and show that 3 divides $n - 4$.

36. *Hint:* Use proof by contradiction. Suppose a, b, and c are odd integers, z is a solution to $ax^2 + bx + c$, and z is rational. Then $z = m'/n'$, for some integers m' *and* n' with $n' \neq 0$. Divide out the greatest common factor of m' and n' (possibly 1) to obtain two integers m and n with no common factor that satisfy the equation $m'/n' = m/n$. Substitute m/n into $ax^2 + bx + c$, and multiply through by n^2. Show that (1) the assumption that m is even leads to a contradiction, and (2) the assumption that n is even leads to a contradiction.

SECTION 4.8

1. The value of $\sqrt{2}$ given by a calculator is an approximation. Calculators can give exact values only for numbers that can be represented using at most the number of decimal digits in the calculator display. In particular, every number in a calculator display is rational, but even many rational numbers cannot be represented exactly. For instance, consider the number formed by writing a decimal point and following it with the first million digits of $\sqrt{2}$. By the discussion in Section 4.2, this number is rational, but you could not infer this from the calculator display.

3. Yes. In fact there are infinitely many rational numbers with the same first trillion digits as $\sqrt{2}$. For instance, if you end the number after the first trillion digits, the result is a finite decimal, which is rational. Repeating the first trillion digits of $\sqrt{2}$ forever would create a repeating decimal, which is rational. Or you could follow the first trillion digits of $\sqrt{2}$ by 012343434. . . , where the digits 34 repeat forever. This is also rational. Try creating other examples.

6. Proof by contradiction: Suppose not. That is, suppose $6 - 7\sqrt{2}$ is rational. *[We must prove a contradiction.]* By definition of rational, there exist integers a and b with $b \neq 0$ with

$$6 - 7\sqrt{2} = \frac{a}{b}.$$

Then

$$\sqrt{2} = \frac{1}{-7}\left(\frac{a}{b} - 6\right)$$ by subtracting 6 from both sides and dividing both sides by -7,

and so $$\sqrt{2} = \frac{a - 6b}{-7b}$$ by the rules of algebra.

But $a - 6b$ and $-7b$ are both integers (since a and b are integers and products and difference of integers are integers), and $-7b \neq 0$ by the zero product property. Hence $\sqrt{2}$ is a ratio of the two integers $a - 6b$ and $-7b$ with $-7b \neq 0$, so $\sqrt{2}$ is a rational number (by definition of rational). This contradicts the fact that $\sqrt{2}$ is irrational, and so the supposition is false and $6 - 7\sqrt{2}$ is irrational.

8. This is false. $\sqrt{4} = 2 = 2/1$, which is rational.

10. Counterexample: Let $x = \sqrt{2}$ and $y = -\sqrt{2}$. Then x and y are irrational, but $x + y = 0 = 0/1$, which is rational.

12. True.

Formal version of the statement: $\forall$ positive real number r, if r is irrational, then $\sqrt{r}$ is irrational.

Proof by contraposition: Suppose r is any positive real number such that $\sqrt{r}$ is rational. *[We must show that r is rational.]* By definition of rational, $\sqrt{r} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Then $r = (\sqrt{r})^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$. But both a^2 and b^2 are integers because they are products of integers, and $b^2 \neq 0$ by the zero product property. Thus r is rational *[as was to be shown]*.

(The statement may also be proved by contradiction.)

16. *Hint:* Can you think of any "nice" integers x and y that are greater than 1 and have the property that $x^2 = y^3$?

19. a. Proof by contradiction: Suppose not. That is, suppose there is an integer n such that $n = 3q_1 + r_1 = 3q_2 + r_2$, where q_1, q_2, r_1, and r_2 are integers, $0 \leq r_1 < 3$, $0 \leq r_2 < 3$, and $r_1 \neq r_2$. By interchanging the labels for r_1 and r_2 if necessary, we may assume that $r_2 > r_1$. Then $3(q_1 - q_2) = r_2 - r_1 > 0$, and because both r_1 and r_2 are less than 3, either $r_2 - r_1 = 1$ or $r_2 - r_1 = 2$. So either $3(q_1 - q_2) = 1$ or $3(q_1 - q_2) = 2$. The first case implies that $3 \mid 1$, and hence, by Theorem 4.4.1, that $3 \leq 1$, and the second case implies that $3 \mid 2$, and hence, by Theorem 4.4.1, that $3 \leq 2$. These results contradict the fact that 3 is greater than both 1 and 2. Thus in either case we have reached a contradiction, which shows that the supposition is false and the given statement is true.

b. Proof by contradiction: Suppose not. That is, suppose there is an integer n such that n^2 is divisible by 3 and n is not divisible by 3. *[We must deduce a contradiction.]* By definition of divisible, $n^2 = 3q$ for some integer q, and by the quotient-remainder theorem and part (a), $n = 3k + 1$ or $n = 3k + 2$ for some integer k.

***Case 1* ($n = 3k + 1$ *for some integer* k):** In this case

$$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1.$$

Let $s = 3k^2 + 2k$. Then $n^2 = 3s + 1$, and s is an integer because it is a sum of products of integers. Thus $n^2 = 3q = 3s + 1$ for some integers q and s, which contradicts the result of part (a).

***Case 2* ($n = 3k + 2$ *for some integer* k):** In this case

$$n^2 = (3k + 2) = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1.$$

Let $t = 3k^2 + 4k + 1$. Then $n^2 = 3t + 1$, and t is an integer because it is a sum of products of integers. Thus there are integers q and t so that $n^2 = 3q = 3t + 1$, which contradicts the result of part (a).

Thus in either case, a contradiction is reached, which shows that the supposition is false and the given statement is true.

c. Proof by contradiction: Suppose not. That is, suppose $\sqrt{3}$ is rational. By definition of rational, $\sqrt{3} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Without loss of generality, assume that a and b have no common factor. (If not, divide both a and b by their greatest common factor to obtain integers a' and b' with the property that a' and b' have no common factor and $\sqrt{3} = \frac{a'}{b'}$. Then redefine $a = a'$ and $b = b$.) Squaring both sides of $\sqrt{3} = \frac{a}{b}$ gives $\sqrt{3} = \frac{a^2}{b^2}$, and multiplying both sides by b^2 gives

$$3b^2 = a^2 (*).$$

Thus a^2 is divisible by 3, and so, by part (b), a is also divisible by 3. By definition of divisibility, then, $a = 3k$ for some integer k, and so

$$a^2 = 9k^2 (**).$$

Substituting equation (**) into equation (*) gives $3b^2 = 9k^2$, and dividing both sides by 3 yields

$$b^2 = 3k^2.$$

Hence b^2 is divisible by 3, and so, by part (b), b is also divisible by 3. Consequently, both a and b are divisible by 3, which contradicts the assumption that a and b have no common factor. Thus the supposition is false, and so $\sqrt{3}$ is irrational.

21. *Hint:* The proof is a generalization of the one given in the solution for exercise 19(a).

22. *Hint:* First prove that for all integers a, if 5 divides a squared then 5 divides a. The rest of the proof is similar to the solution for exercise 19(c).

23. *Hint:* This statement is true. If $a^2 - 3 = 9b$, then $a^2 = 9b + 3 = 3(3b + 1)$, and so a^2 is divisible by 3. Hence, by exercise 19(b), a is divisible by 3. Thus $a^2 = (3c)^2$ for some integer c.

24. Proof by contradiction: Suppose not. That is, suppose $\sqrt{2}$ is rational. *[We will show that this supposition leads to a contradiction.]* By definition of rational, we may write $\sqrt{2} = a/b$ for some integers a and b with $b \neq 0$. Then $2 = a^2/b^2$, and so $a^2 = 2b^2$. Consider the prime factorizations for a^2 and for $2b^2$. By the unique factorization of integers theorem, these factorizations are unique except for the order in which the factors are written. Now because every prime factor of a occurs twice in the prime factorization of a^2, the prime factorization of a^2 contains an even number of 2's. (If 2 is a factor of a, then this even number is positive, and if 2 is not a factor of a, then this even number is 0.) On the other hand, because every prime factor of b occurs twice in the prime factorization of b^2, the prime factorization of $2b^2$ contains an odd number of 2's. Therefore, the equation

$a^2 = 2b^2$ cannot be true. So the supposition is false, and hence $\sqrt{2}$ is irrational.

26. *Hint:* One solution uses only Theorem 4.8.1. Another uses the result of exercise 25 that $\sqrt{6}$ is irrational.

28. *Hint:* Divide $2\cdot3\cdot5\cdot7+1$ by each of 2, 3, 5, and 7, using the quotient-remainder theorem.

29. *Hint:* You can deduce that $p = 3$.

30. a. *Hint:* For example, $N_4 = 2\cdot3\cdot5\cdot7+1 = 211$.

32. *Hint:* By Theorem 4.2.4 (divisibility by a prime) there is a prime number p such that $p \mid (n!-1)$. Show that the supposition that $p \le n$ leads to a contradiction. It will then follow that $n < p < n!$.

33. *Hint:* Every odd integer can be written as $4k+1$ or as $4k+3$ for some integer k. (Why?) If $p_1 p_2 \ldots p_n + 1 = 4k+1$, then $4 \mid p_1 p_2 \ldots p_n$. Is this possible?

34. a. *Hint:* Prove the contrapositive: If for some integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has a positive integer solution, then for some prime number $p > 2$, $x^p + y^p = z^p$ has a positive integer solution. Note that if $n = kp$, then $x^n = x^{kp} = (x^k)^p$.

35. Existence proof: When $n = 2$, then $n^2 - 1 = 3$, which is prime. Hence there exists a prime number of the form $n^2 - 1$, where n is an integer and $n \ge 2$.

Uniqueness proof (by contradiction): Suppose to the contrary that m is another integer satisfying the given conditions. That is, $m > 2$ and $m^2 - 1$ is prime. *[We must derive a contradiction.]* Factor $m^2 - 1$ to obtain $m^2 - 1 = (m-1)(m+1)$. But $m > 2$, and so $m - 1 > 1$ and $m + 1 > 1$. Hence $m^2 - 1$ is not prime, which is a contradiction. *[This contradiction shows that the supposition is false, and so there is no other integer $m > 2$ such that $n^2 - 1$ is prime.]*

Uniqueness proof (direct): Suppose m is any integer such that $m \ge 2$ and $m^2 - 1$ is prime. *[We must show that $m = 2$.]* By factoring, $m^2 - 1 = (m-1)(m+1)$. Since $m^2 - 1$ is prime, either $m - 1 = 1$ or $m + 1 = 1$. But $m + 1 \ge 2 + 1 = 3$. Hence, by elimination, $m - 1 = 1$, and so $m = 2$.

37. Proof (by contradiction): Suppose not. That is, suppose there are two distinct real numbers a_1 and a_2 such that for all real numbers r,

$$(1)\ a_1 + r = r \quad \text{and} \quad (2)\ a_2 + r = r.$$

Then

$$a_1 + a_2 = a_2 \quad \text{by (1) with} \quad r = a_2$$

and

$$a_2 + a_1 = a_1 \quad \text{by (2) with} \quad r = a_1.$$

It follows that

$$a_2 = a_1 + a_2 = a_2 + a_1 = a_1,$$

which implies that $a_2 = a_1$. But this contradicts the supposition that a_1 and a_2 are distinct. *[Thus the supposition is false and there is at most one real number a such that $a + r = r$ for all real numbers r.]*

Proof (direct): Suppose a_1 and a_2 are real numbers such that for all real numbers r,

$$(1)\ a_1 + r = r \quad \text{and} \quad (2)\ a_2 + r = r.$$

Then

$$a_1 + a_2 = a_2 \text{ by (1)} \quad \text{with} \quad r = a_2$$

and

$$a_2 + a_1 = a_1 \quad \text{by (2) with} \quad r = a_1.$$

It follows that

$$a_2 = a_1 + a_2 = a_2 + a_1 = a_1.$$

Hence $a_2 = a_1$. *[Thus there is at most one real number a such that $a + r = r$ for all real numbers r.]*

SECTION 4.9

1.

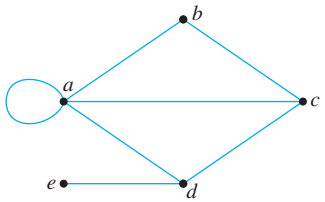
vertex	v_1	v_2	v_3	v_4	v_5	v_6
degree	3	2	4	2	1	0

Total degree $= 3 + 2 + 4 + 2 + 1 = 12$

$$\#\text{ of edges} = 6 = \left(\frac{1}{2}\right)12 = \text{one-half of the total degree}$$

3. The total degree of the graph is $0 + 2 + 2 + 3 + 9 = 16$, , so, by the handshake theorem (Theorem 4.9.1), the number of edges is $16/2 = 8$.

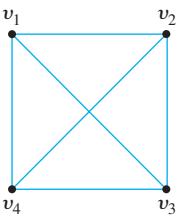
5. One such graph is



6. If there were a graph with four vertices of degree 1, 2, 3, and 3, then its total degree would be 9, which is odd. But by Corollary 4.9.2, the total degree of the graph must be even. *[This is a contradiction.]* Hence there is no such graph. (Alternatively, if there were such a graph, it would have an odd number of vertices of odd degree. But by Proposition 4.9.3 this is impossible.)

9. Suppose there were a simple graph with four vertices of degrees 1, 2, 3, and 4. Then the vertex of degree 4 would have to be connected by edges to four distinct vertices other than itself because of the assumption that

the graph is simple (and hence has no loops or parallel edges). This contradicts the assumption that the graph has four vertices in total. Hence there is no simple graph with four vertices of degrees 1, 2, 3, and 4.

12. 

14. a. Define a graph G by letting each vertex represent a person at the party and drawing an edge between each pair of people who knew each other before the party. Let x be the number of people who knew three other people before the party.

Then the total degree of the graph

$$= 2\cdot 1 + 5\cdot 2 + x\cdot 3 = 12 + 3x$$

because 2 people knew 1 other person before the party, 5 people knew 2 other people before the party, and x people knew 3 other people before the party. In addition, since a total of 15 pairs of people knew each other before the party, the graph has 15 edges. By the handshake theorem (Theorem 4.9.1), the total degree is twice the number of edges. Hence the total degree of the graph $= 2\cdot 15 = 30$.

It follows that $12 + 3x = 30$. Thus

$$3x = 30 - 12 = 18, \quad \text{and so} \quad x = \frac{18}{3} = 6.$$

In other words, 6 people at the party knew 3 other people before the party.

b. Now the total number of people at the party is the sum of the number who knew 1 other person before the party, plus the number who knew 2 other people before the party, plus the number who knew 3 other people before the party. Therefore, the number of people at the party $= 2 + 5 + 6 = 13$.

16. a. Suppose that, in a group of 15 people, each person had exactly three friends. Then you could draw a graph representing each person by a vertex and connecting two vertices by an edge if the corresponding people were friends. But such a graph would have 15 vertices, each of degree 3, for a total degree of 45. This would contradict the fact that the total degree of any graph is even. Hence the supposition must be false, and in a group of 15 people it is not possible for each to have exactly three friends.

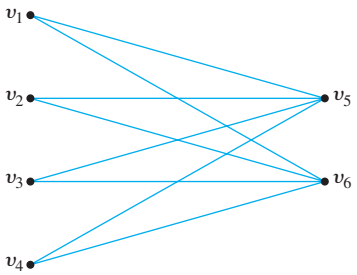
19. *Hint:* Let t be the total degree of the graph, let $d_{\min}$ be the minimum degree of any vertex in G, and let $d_{\max}$ be the maximum degree of any vertex in G.

21. a. Yes. Let G be a simple graph with n vertices and let v be a vertex of G. Since G has no parallel edges, v can be joined by at most a single edge to each of the $n - 1$ other vertices of G, and since G has no loops, v cannot be joined to itself. Therefore, the maximum degree of v is $n - 1$.

b. No. Suppose there is a simple graph with four vertices, all of which have different degrees. By part (a), no vertex can have degree greater than three, and of course, no vertex can have degree less than 0. Therefore, the only possible degrees of the vertices are 0, 1, 2, and 3. Since all four vertices have different degrees, there is one vertex with each degree. But then the vertex of degree 3 is connected to all the other vertices, which contradicts the fact that one of the vertices has degree 0. Hence the supposition is false, and there is no simple graph with four vertices each of which has a different degree.

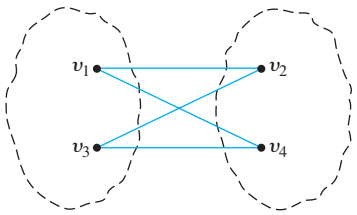
22. *Hint:* Use the result of exercise 21, part (c).

23. a. $K_{4,2}$:



23. d. If $n \neq m$, the vertices of $K_{m,n}$ are divided into two groups: one of size m and the other of size n. Every vertex in the group of size m has degree n because each is connected to every vertex in the group of size n. So $K_{m,n}$ has m vertices of degree n. Similarly, every vertex in the group of size n has degree m because each is connected to every vertex in the group of size m. So $K_{m,n}$ has n vertices of degree m. Note that if $n = m$, then all $n + m = 2n$ vertices have the same degree, namely, n.

24. a. This graph is bipartite



b. Suppose this graph is a bipartite. Then the vertex set can be partitioned into two mutually disjoint subsets such that vertices in each subset are

connected by edges only to vertices in the other subset and not to vertices in the same subset. Now v_1 is in one subset of the partition, say, V_1. Since v_1 is connected by edges to v_2 and v_3 both v_2 and v_3 must be in the other subset, V_2. But v_2 and v_3 are connected by an edge to each other. This contradicts the fact that no vertices in V_2 are connected by edges to other vertices in V_2. Hence the supposition is false, and so the graph is not bipartite.

SECTION 4.10

1. $z = 0$

3. a. $z = 18$

4. Trace table:

i	0	1	2	3
a	2	7	22	67

After execution: $a = 67$

6.

	Iteration Number			
	0	1	2	3
a	26			
d	7			
q	0	1	2	3
r	26	19	12	5

8. a.

A	69	19	9	
q	2			
d		1		
n			1	
p				4

9. gcd(27, 72) = 9

10. gcd(5, 9) = 1

13. Divide the larger number, 1,188, by the smaller, 385, to obtain a quotient of 3 and a remainder of 33. Next divide 385 by 33 to obtain a quotient of 11 and a remainder of 22. Then divide 33 by 22 to obtain a quotient of 1 and a remainder of 11. Finally, divide 22 by 11 to obtain a quotient of 2 and a remainder of 0. Thus, by Lemma 4.10.2, gcd(1188, 385) = gcd(385, 33) = gcd(33, 22) = gcd(22, 11) = gcd(11, 0), and by Lemma 4.10.1, gcd(11, 0) = 11. So gcd(1188, 385) = 11.

14. Divide the larger number, 1,177, by the smaller, 509, to obtain a quotient of 2 and a remainder of 159. Next divide 509 by 159 to obtain a quotient of 3 and a remainder of 32. Next divide 159 by 32 to obtain a quotient of 4 and a remainder of 31. Then divide 32 by 31 to obtain a quotient of 1 and a remainder of 1. Finally, divide 31 by 1 to obtain a quotient of 31 and a remainder of 0. Thus, by Lemma 4.10.2, gcd(1177, 509) = gcd(509, 159) = gcd(159, 32) = gcd(32, 31) = gcd(31, 1) = gcd(1, 0), and by Lemma 4.10.1, gcd(1, 0) = 1. So gcd(1177, 509) = 1.

17.

A	1,001					
B	871					
r		130	91	39	13	0
b	871	130	91	39	13	0
a	1,001	871	130	91	39	13
gcd						13

20.

A	4,617								
B	2,563								
a	4,617	2,563	2,054	509	18	5	3	2	1
b	2,563	2,054	509	18	5	3	2	1	0
r	2,563	2,054	509	18	5	3	2	1	0
gcd									1

The table shows that the greatest common divisor of 4,617 and 2,563 is 1, and so these integers are relatively prime.

22. *Hint:* Divide the proof into two parts. In part 1 suppose a and b are any positive integers such that $a|b$, and derive the conclusion that $\gcd(a, b) = a$. To do this, note that because it is also the case that $a|a$, a is a common divisor of a and b. Thus, by definition of greatest common divisor, a is less than or equal to the greatest common divisor of a and b. In symbols, $a \le \gcd(a, b)$. Then show that $a \ge \gcd(a, b)$ by using Theorem 4.4.1. In part 2 of the proof, suppose a and b are positive integers such that $\gcd(a, b) = a$ and deduce that $a|b$.

25. a. *Hint 1:* If $a = dq - r$, then $-a = -dq + r = -dq - d + d - r = d(-q - 1) + (d - r)$.

Hint 2: If $0 \le r < d$, then $0 \ge -r > -d$. Add d to all parts of this inequality and see what results.

26. a. Proof: Suppose a, d, q, and r are integers such that $a = dq + r$ and $0 \le r < d$. *[We must show that* $q = \lfloor \frac{a}{d} \rfloor$ *and* $r = a - d\lfloor \frac{a}{d} \rfloor$*.]* Solving $a = dq + r$ for r gives $r = a - dq$, and substituting into $0 \le r < d$ gives $0 \le a - dq < d$. Add dq to both sides to obtain $dq \le a < d + dq = d(q + 1)$. Then divide through by d to obtain $q \le \frac{a}{d} < q + 1$. Therefore, by definition of floor, $\lfloor \frac{a}{d} \rfloor = q$. Finally, substitution into $a = dq + r$ gives $a = d\lfloor \frac{a}{d} \rfloor + r$, and subtracting $d\lfloor \frac{a}{d} \rfloor$ from both sides yields $r = a - d\lfloor \frac{a}{d} \rfloor$ *[as was to be shown].*

27. b.

	Iteration Number				
	0	1	2	3	4
a	630	294	294	252	210
b	336	336	42	42	42
gcd					

	Iteration Number				
	5	6	7	8	9
a	168	126	84	42	0
b	42	42	42	42	42
gcd					42

28. a. $\text{lcm}(12, 18) = 36$

29. Proof: *Part 1:* Let a and b be positive integers, and suppose $d = \gcd(a, b) = \text{lcm}(a, b)$. By definition of greatest common divisor and least common multiple, $d > 0$, $d|a$, $d|b$, $a|d$, and $b|d$. Thus, in particular, $a = dm$ and $d = an$ for some integers m and n. By substitution, $a = dm = (an)m = anm$. Dividing both sides by a gives $1 = nm$. But the only divisors of 1 are 1 and -1 (Theorem 4.4.2), and so $m = n = \pm 1$. Since both a and d are positive, $m = n = 1$, and hence $a = d$. Similar reasoning shows that $b = d$ also, and so $a = b$.

Part 2: Given any positive integers a and b such that $a = b$, we have $\gcd(a, b) = \gcd(a, a) = a$ and $\text{lcm}(a, b) = \text{lcm}(a, a) = a$, and hence $\gcd(a, b) = \text{lcm}(a, b)$.

32. *Hint:* Divide the proof into two parts. In part 1, suppose a and b are any positive integers, and deduce that

$$\gcd(a, b) \cdot \text{lcm}(a, b) \le ab.$$

Derive this result by showing that $\text{lcm}(a, b) \le \frac{ab}{\gcd(a, b)}$. To do this, show that $\frac{ab}{\gcd(a, b)}$ is a multiple of both a and b. For instance, to see that $\frac{ab}{\gcd(a, b)}$ is a multiple of b, note that because $\gcd(a, b)$ divides a, $a = \gcd(a, b) \cdot k$ for some integer k, and thus $ab = \gcd(a, b) \cdot kb$. Divide both sides by $\gcd(a, b)$ to obtain $\frac{ab}{\gcd(a, b)} = kb$. But since k is an integer, this equation implies that $\frac{ab}{\gcd(a, b)}$ is a multiple of b. The argument that $\frac{ab}{\gcd(a, b)}$ is a multiple of a is almost identical. In part 2 of the proof, use the definition of least common multiple to show that $\frac{ab}{\text{lcm}(a, b)}|a$ and $\frac{ab}{\text{lcm}(a, b)}|b$. Conclude that $\frac{ab}{\text{lcm}(a, b)} \le \gcd(a, b)$ and hence that $ab \le \gcd(a, b) \cdot \text{lcm}(a, b)$.

SECTION 5.1

1. $\frac{1}{11}, \frac{2}{12}, \frac{3}{13}, \frac{4}{14}$ **3.** $1, -\frac{1}{3}, \frac{1}{9}, -\frac{1}{27}$ **5.** 0, 0, 2, 2

8. $g_1 = \lfloor \log_2 1 \rfloor = 0$

$g_2 = \lfloor \log_2 2 \rfloor = 1, \quad g_3 = \lfloor \log_2 3 \rfloor = 1$

$g_4 = \lfloor \log_2 4 \rfloor = 2, \quad g_5 = \lfloor \log_2 5 \rfloor = 2$

$g_6 = \lfloor \log_2 6 \rfloor = 2, \quad g_7 = \lfloor \log_2 7 \rfloor = 2$

$g_8 = \lfloor \log_2 8 \rfloor = 3, \quad g_9 = \lfloor \log_2 9 \rfloor = 3$

$g_{10} = \lfloor \log_2 10 \rfloor = 3, \quad g_{11} = \lfloor \log_2 11 \rfloor = 3$

$g_{12} = \lfloor \log_2 12 \rfloor = 3, \quad g_{13} = \lfloor \log_2 13 \rfloor = 3$

$g_{14} = \lfloor \log_2 14 \rfloor = 3, \quad g_{15} = \lfloor \log_2 15 \rfloor = 3$

When n is an integral power of 2, g_n is the exponent of that power. For instance, $8 = 2^3$ and $g_8 = 3$. More generally, if $n = 2^k$, where k is an integer, then $g_n = k$. All terms of the sequence from g_{2^k} up to, but not including, $g_{2^{k+1}}$ have the same value, namely k. For instance, all terms of the sequence from g_8 through g_{15} have the value 3.

Exercises 10–16 have more than one correct answer.

10. $a_n = (-1)^n$, where n is an integer and $n \ge 1$

11. $a_n = (n - 1)(-1)^n$, where n is an integer and $n \ge 1$

12. $a_n = \dfrac{n}{(n + 1)^2}$, where n is an integer and $n \ge 1$

14. $a_n = \dfrac{n^2}{3^n}$, where n is an integer and $n \ge 1$

18. a. $2+3+(-2)+1+0+(-1)+(-2)=1$

b. $a_0=2$

c. $a_2+a_4+a_6=-2+0+(-2)=-4$

d. $2\cdot 3\cdot(-2)\cdot 1\cdot 0\cdot(-1)\cdot(-2)=0$

19. $2+3+4+5+6=20$ **20.** $2^2\cdot 3^2\cdot 4^2=576$

23. $1(1+1)=2$

27. $\left(\frac{1}{1}-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+\left(\frac{1}{4}-\frac{1}{5}\right)+\left(\frac{1}{5}-\frac{1}{6}\right)+\frac{1}{6}-\frac{1}{7}=1-\frac{1}{7}=\frac{6}{7}$

29. $(-2)^1+(-2)^2+(-2)^3+\cdots+(-2)^n=-2+2^2-2^3+\cdots+(-1)^n2^n$

31. $\sum_{k=0}^{n+1}\frac{1}{k!}=\frac{1}{0!}+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{(n+1)!}$

33. $\frac{1}{1^2}=1$

35. $\left(\frac{1}{1+1}\right)\left(\frac{2}{2+1}\right)\left(\frac{3}{3+1}\right)=\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{3}{4}\right)=\frac{1}{4}$

37. $\sum_{i=1}^{k}i^3+(k+1)^3=\sum_{i=1}^{k+1}i^3$

39. *Hint:* $n+2=(n+1)+1$.

40. $\sum_{i=1}^{k+1}i(i!)=\sum_{i=1}^{k}i(i!)+(k+1)(k+1)!$

Exercises 43–52 have more than one correct answer.

43. $\sum_{k=1}^{7}(-1)^{k+1}k^2$ or $\sum_{k=0}^{6}(-1)^k(k+1)^2$

46. $\sum_{j=2}^{6}\frac{(-1)^j j}{(j+1)(j+2)}$ or $\sum_{k=3}^{7}\frac{(-1)^{k+1}(k-1)}{k(k+1)}$

47. $\sum_{i=0}^{5}(-1)^i r^i$ **49.** $\sum_{k=1}^{n}k^3$

51. $\sum_{i=0}^{n-1}(n-i)$

53. When $k=0$, then $i=1$. When $k=5$, then $i=6$. Since $i=k+1$, then $k=i-1$. Thus,

$$k(k-1)=(i-1)((i-1)-1)=(i-1)(i-2),$$

and so

$$\sum_{k=0}^{5}k(k-1)=\sum_{i=1}^{6}(i-1)(i-2)$$

55. When $i=1$, then $j=0$. When $i=n+1$, then $j=n$. Since $j=i-1$, then $i=j+1$. Thus,

$$\frac{(i-1)^2}{i\cdot n}=\frac{((j+1)-1)^2}{(j+1)\cdot n}=\frac{j^2}{jn+n}.$$

(Note that n has the same value in each term of the sum.)

So $\sum_{i=1}^{n+1}\frac{(i-1)^2}{i\cdot n}=\sum_{j=0}^{n}\frac{j^2}{jn+n}$.

56. When $i=3$, then $j=2$. When $i=n$, then $j=n-1$. Since $j=i-1$, then $i=j+1$. Thus,

$$\sum_{i=3}^{n}\frac{i}{i+n-1}=\sum_{j=2}^{n-1}\frac{j+1}{(j+1)+n-1}=\sum_{j=2}^{n-1}\frac{j+1}{j+n}.$$

59. $\sum_{k=1}^{n}[3(2k-3)+(4-5k)]=\sum_{k=1}^{n}[(6k-9)+(4-5k)]=\sum_{k=1}^{n}(k-5)$

62. $\frac{4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 1}=4$

65. $\frac{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}=n$

66. $\frac{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n+1)n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}=\frac{1}{n(n+1)}$

68. $\frac{[(n+1)n(n-1)(n-2)\cdots 3\cdot 2\cdot 1]^2}{[n(n-1)(n-2)\cdots 3\cdot 2\cdot 1]^2}=(n+1)^2$

69. $\frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)(n-k-1)\cdots 2\cdot 1}{(n-k)(n-k-1)\cdots 2\cdot 1}=n(n-1)(n-2)\cdots(n-k+1)$

71. $\binom{5}{3}=\frac{5!}{(3!)(5-3)!}=\frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{(3\cdot 2\cdot 1)(2\cdot 1)}=10$

73. $\binom{3}{0}=\frac{3!}{(0!)(3-0)!}=\frac{3!}{(1)(3!)}=1$

75. $\binom{n}{n-1}=\frac{n!}{(n-1)!(n-(n-1))!}=\frac{n(n-1)!}{(n-1)!(n-n+1)!}=\frac{n}{1}=n$

77. a. Proof: Let n be an integer such that $n\geq 2$. By definition of factorial,

$$n!=\begin{cases}2\cdot 1 & \text{if } n=2\\ 3\cdot 2\cdot 1 & \text{if } n=3\\ n\cdot(n-1)\cdot\cdots 2\cdot 1 & \text{if } n>3.\end{cases}$$

In each case, $n!$ has a factor of 2, and so $n! = 2k$ for some integer k. Then

$$\begin{aligned} n! + 2 &= 2k + 2 && \text{by substitution} \\ &= 2(k+1) && \text{by factoring out the 2.} \end{aligned}$$

Since $k+1$ is an integer, $n!+2$ is divisible by 2 *[as was to be shown]*.

c. *Hint:* Consider the sequence $m!+2$, $m!+3$, $m!+4$, . . ., $m!+m$.

78. Proof: Suppose n and r are nonnegative integers with $r+1 \le n$. The right-hand side of the equation to be shown is

$$\begin{aligned} \frac{n-r}{r+1}\cdot\binom{n}{r} &= \frac{n-r}{r+1}\cdot\frac{n!}{r!(n-r)!} \\ &= \frac{n-r}{r+1}\cdot\frac{n!}{r!(n-r)\cdot(n-r-1)!} \\ &= \frac{n!}{(r+1)!\cdot(n-r-1)!} \\ &= \frac{n!}{(r+1)!\cdot(n-(r+1))!} \\ &= \binom{n}{r+1}, \end{aligned}$$

which is the left-hand side of the equation to be shown.

80. a. $m-1$, $sum + a[i+1]$

81.

```
                    0    remainder = r[6] = 1
                2 | 1    remainder = r[5] = 0
            2 | 2        remainder = r[4] = 1
        2 | 5            remainder = r[3] = 1
    2 | 11                remainder = r[2] = 0
2 | 22                    remainder = r[1] = 1
2 | 45                    remainder = r[0] = 0
2 | 90
```

Hence $90_{10} = 1011010_2$.

84.

a	23					
i	0	1	2	3	4	5
q	23	11	5	2	1	0
r[0]		1				
r[1]			1			
r[2]				1		
r[3]					0	
r[4]						1

88.

```
                0    remainder 1  = r[2] = 1_16
            16 | 1    remainder 1  = r[1] = 1_16
        16 | 17       remainder 15 = r[0] = F_16
16 | 287
```

Hence $287_{10} = 11F_{16}$.

SECTION 5.2

1. a. The statement in part (a) is true because if $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = \frac{1}{3}$ then

$$\begin{aligned} &\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right) \\ &= \frac{1}{3}\left(1-\frac{1}{4}\right) = \frac{1}{3}\cdot\frac{3}{4} = \frac{1}{4}. \end{aligned}$$

2. a. $P(1)$ is the equation $1 = 1^2$, which is true.

b. $P(k)$ is the equation $1+3+5+\cdots+(2k-1) = k^2$.

c. $P(k+1)$ is the equation $1+3+5+\cdots+(2(k+1)-1) = (k+1)^2$

d. In the inductive step, show that if k is any integer for which $1+3+5+\cdots+(2k-1) = k^2$ is true, then $1+3+5+\cdots+(2(k+1)-1) = (k+1)^2$ is also true.

3. a. $P(1)$ is "$1^2 = \frac{1\cdot(1+1)\cdot(2\cdot1+1)}{6}$." $P(1)$ is true because the left-hand side equals $1^2 = 1$ and the right-hand side equals $\frac{1\cdot(1+1)\cdot(2+1)}{6} = \frac{2\cdot3}{6} = 1$ also.

5. a. 1^2

b. k^2

c. $1+3+5+\cdots+[(2(k+1)-1]$

d. $(k+1)^2$

e. the odd integer just before $2k+1$ is $2k-1$

f. inductive hypothesis

6. Proof: For the given statement, the property $P(n)$ is the equation

$$2+4+6+\cdots+2n = n^2+n. \quad \leftarrow P(n)$$

Show that P(1) is true:

To prove $P(1)$, we must show that when 1 is substituted into the equation in place of n, the left-hand side equals the right-hand side. But when 1 is substituted for n, the left-hand side is the sum of all the even integers from 2 to $2\cdot1$, which is just 2, and the right-hand side is 1^2+1, which also equals 2. Thus $P(1)$ is true.

Show that for every integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true:

Let k be any integer with $k \geq 1$, and suppose $P(k)$ is true. That is, suppose

$2+4+6+\cdots+2k = k^2+k.$ ← $P(k)$ inductive hypothesis

We must show that $P(k+1)$ is true. That is, we must show that

$$2+4+6+\cdots+2(k+1) = (k+1)^2+(k+1).$$

Because $(k+1)^2+(k+1) = k^2+2k+1+k+1 = k^2+3k+2$, this is equivalent to showing that

$2+4+6+\cdots+2(k+1) = k^2+3k+2.$ ← $P(k+1)$

Now the left-hand side of $P(k+1)$ is

$$\begin{aligned} &2+4+6+\cdots+2(k+1) \\ &\quad = 2+4+6+\cdots+2k+2(k+1) && \text{by making the next-to-last term explicit} \\ &\quad = (k^2+k)+2(k+1) && \text{by substitution from the inductive hypothesis} \\ &\quad = k^2+3k+2 && \text{by algebra,} \end{aligned}$$

and this is the right-hand side of $P(k+1)$. Hence $P(k+1)$ is true.

[Since both the basis step and the inductive step have been proved, $P(n)$ is true for every integer $n \geq 1$.]

8. Proof: For the given statement, the property $P(n)$ is the equation

$$1+2+2^2+\cdots+2^n = 2^{n+1}-1. \quad \leftarrow P(n)$$

Show that $P(0)$ is true:

The left-hand side of $P(0)$ is 1, and the right-hand side is $2^{0+1}-1 = 2-1 = 1$ also. Thus $P(0)$ is true.

Show that for every integer $k \geq 0$, if $P(k)$ is true then $P(k+1)$ is true:

Let k be any integer with $k \geq 0$, and suppose $P(k)$ is true. That is, suppose

$1+2+2^2+\cdots+2^k = 2^{k+1}-1.$ ← $P(k)$ inductive hypothesis

We must show that $P(k+1)$ is true. That is, we must show that

$$1+2+2^2+\cdots+2^{k+1} = 2^{(k+1)+1}-1,$$

or, equivalently,

$$1+2+2^2+\cdots+2^{k+1} = 2^{k+2}-1. \quad \leftarrow P(k+1)$$

Now the left-hand side of $P(k+1)$ is

$$\begin{aligned} &1+2+2^2+\cdots+2^{k+1} \\ &\quad = 1+2+2^2+\cdots+2^k+2^{k+1} && \text{by making the next-to-last term explicit} \\ &\quad = (2^{k+1}-1)+2^{k+1} && \text{by substitution from the inductive hypothesis} \\ &\quad = 2\cdot 2^{k+1}-1 && \text{by combining like terms} \\ &\quad = 2^{k+2}-1 && \text{by the laws of exponents,} \end{aligned}$$

and this is the right-hand side of $P(k+1)$. Hence the property is true for $n = k+1$.

[Since both the basis step and the inductive step have been proved, $P(n)$ is true for every integer $n \geq 0$.]

10. Proof: For the given statement, the property is the equation

$$1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}. \quad \leftarrow P(n)$$

Show that $P(1)$ is true:

The left-hand side of $P(1)$ is $1^2 = 1$, and the right-hand side is $\frac{1(1+1)(2\cdot 1+1)}{6} = \frac{2\cdot 3}{6} = 1$ also. Thus $P(1)$ is true.

Show that for every integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true:

Let k be any integer with $k \geq 1$, and suppose $P(k)$ is true. That is, suppose

$$1^2+2^2+3^2+\cdots+k^2 = \frac{k(k+1)(2k+1)}{6}. \quad \leftarrow P(k) \text{ inductive hypothesis}$$

We must show that $P(k+1)$ is true. That is, we must show that

$$1^2+2^2+3^2+\cdots+(k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6},$$

or, equivalently,

$$1^2+2^2+3^2+\cdots+(k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}. \quad \leftarrow P(k+1)$$

Now the left-hand side of $P(k+1)$ is

$$1^2+2^2+3^2+\cdots+(k+1)^2$$
$$=1^2+2^2+3^2+\cdots+k^2+(k+1)^2 \qquad \text{by making the next-to-last term explicit by substitution from the inductive hypothesis}$$
$$=\frac{k(k+1)(2k+1)}{6}+(k+1)^2$$
$$=\frac{k(k+1)(2k+1)}{6}+\frac{6(k+1)^2}{6} \qquad \text{because } \tfrac{6}{6}=1$$
$$=\frac{k(k+1)(2k+1)+6(k+1)^2}{6} \qquad \text{by adding fractions}$$
$$=\frac{k(k+1)[k(2k+1)+6(k+1)]}{6} \qquad \text{by factoring out } (k+1)$$
$$=\frac{(k+1)(2k^2+7k+6)}{6} \qquad \text{by multiplying out and combining like terms}$$
$$=\frac{(k+1)(k+2)(2k+3)}{6} \qquad \text{because } (k+2)(2k+3)=2k^2+7k+6,$$

and this is the right-hand side of $P(k+1)$. Hence the property is true for $n=k+1$.

[Since both the basis step and the inductive step have been proved, $P(n)$ is true for every integer $n \geq 1$.]

13. Proof: For the given statement, the property $P(n)$ is the equation

$$\sum_{i=1}^{n-1} i(i+1)=\frac{n(n-1)(n+1)}{3}. \quad \leftarrow P(n)$$

Show that P(2) is true:

The left-hand side of $P(2)$ is $\sum_{i=1}^{1} i(i+1)=1\cdot(1+1)=2$, and the right-hand side is $\frac{2(2-1)(2+1)}{3}=\frac{6}{3}=2$ also. Thus $P(2)$ is true.

Show that for every integer $k \geq 2$, if $P(k)$ is true then $P(k+1)$ is true:

Let k be any integer with $k \geq 2$, and suppose $P(k)$ is true. That is, suppose

$$\sum_{i=1}^{k-1} i(i+1)=\frac{k(k-1)(k+1)}{3} \quad \leftarrow P(k) \text{ inductive hypothesis}$$

We must show that $P(k+1)$ is true. That is, we must show that

$$\sum_{i=1}^{(k+1)-1} i(i+1)=\frac{(k+1)((k+1)-1)((k+1)+1)}{3},$$

or, equivalently,

$$\sum_{i=1}^{k} i(i+1)=\frac{(k+1)k(k+2)}{3}. \quad \leftarrow P(k+1)$$

Now the left-hand side of $P(k+1)$ is

$$\sum_{i=1}^{k} i(i+1)$$
$$=\sum_{i=1}^{k-1} i(i+1)+k(k+1) \qquad \text{by writing the last term separately}$$
$$=\frac{k(k-1)(k+1)}{3}+k(k+1) \qquad \text{by substitution from the inductive hypothesis}$$
$$=\frac{k(k-1)(k+1)}{3}+\frac{3k(k+1)}{3} \qquad \text{because } \tfrac{3}{3}=1$$
$$=\frac{k(k-1)(k+1)+3k(k+1)}{3} \qquad \text{by adding the fractions}$$
$$=\frac{k(k+1)[(k-1)+3]}{3} \qquad \text{by factoring out } k(k+1)$$
$$=\frac{k(k+1)(k+2)}{3} \qquad \text{by algebra,}$$

and this is the right-hand side of $P(k+1)$. Hence $P(k+1)$ is true.

[Since both the basis step and the inductive step have been proved, $P(n)$ is true for every integer $n \geq 2$.]

15. *Hint:* To prove the basis step, show that $\sum_{i=1}^{1} i(i!)=(1+1)!-1$. To prove the inductive step, suppose that k is any integer such that $k \geq 1$ and $\sum_{i=1}^{k} i(i!)=(k+1)!-1$, and show that $\sum_{i=1}^{k+1} i(i!)=(k+2)!-1$. Note that $[(k+1)!-1]+(k+1)[(k+1)!]=(k+1)![1+(k+1)]-1$.

20. $4+8+12+16+\cdots+200=4(1+2+3+\cdots+50)=4\left(\frac{50\cdot 51}{2}\right)=5{,}100$

22. a. $3+4+5+6+\cdots+1000$
$$=(1+2+3+4+\cdots+1000)-(1+2)$$
$$=\left(\frac{1000\cdot 1001}{2}\right)-3=500{,}497$$

b. $3+4+5+6+\cdots+m$
$$=(1+2+3+4+\cdots+m)-(1+2)$$
$$=\frac{m(m+1)}{2}-3=\frac{m^2+m}{2}-\frac{6}{2}$$
$$=\frac{m^2+m-6}{2}$$

24. $\dfrac{(k-1)((k-1)+1)}{2} = \dfrac{k(k-1)}{2}$

25. a. $\dfrac{2^{26}-1}{2-1} = 2^{26}-1 = 67{,}108{,}863$

b. $2+2^2+2^3+\cdots+2^{26}$
$= 2(1+2+2^2+\cdots+2^{25})$
$= 2\cdot(67108863)$ by part (a)
$= 134{,}217{,}726$

c. *Solution 1:*
$2+2^2+2^3+\cdots+2^n$
$= 2(1+2+2^2+2^3+\cdots+2^{n-1})$
$= 2\left(\dfrac{2^{(n-1)+1}-1}{2-1}\right) = \left(\dfrac{2^n-1}{2-1}\right)-2 = 2^{n+1}-2$

Solution 2:
$2+2^2+2^3+\cdots+2^n = (1+2+2^2+2^3+\cdots+2^n)-1$
$= \dfrac{2^{n+1}-1}{2-1}-1 = 2^{n+1}-2$

28. $\dfrac{\left(\frac{1}{2}\right)^{n+1}-1}{\frac{1}{2}-1} = \dfrac{\frac{1}{2^{n+1}}-1}{-\frac{1}{2}} = \left(\dfrac{1}{2^{n+1}}-1\right)(-2)$
$= -\dfrac{2}{2^{n+1}}+2 = 2-\dfrac{1}{2^n}$

30. *General formula:* For every integer $n \geq 1$,
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}$$

Proof (by mathematical induction): Let the property $P(n)$ be the equation
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}.$$

Show that P(1) is true:

The left-hand side of $P(1)$ equals $\frac{1}{1\cdot 3}$, and the right-hand side equals $\frac{1}{2\cdot 1+1}$. But both of these equal $\frac{1}{3}$, so $P(1)$ is true.

Show that for each integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true:

Suppose that k is any integer with $k \geq 1$, and
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2k-1)(2k+1)} = \frac{k}{2k+1}.$$ ← $P(k)$ inductive hypothesis

We must show that
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2(k+1)-1)(2(k+1)+1)} = \frac{k+1}{2(k+1)+1}.$$
or, equivalently,
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2k+1)(2k+3)} = \frac{k+1}{2k+3}.$$ ← $P(k+1)$

Now the left-hand side of $P(k+1)$ is
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2k+1)(2k+3)}$$
$$= \frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2k-1)(2k+1)} + \frac{1}{(2k+1)(2k+3)}$$
$$= \frac{k}{2k+1}+\frac{1}{(2k+1)(2k+3)}$$ by inductive hypothesis
$$= \frac{k(2k+3)}{(2k+1)(2k+3)}+\frac{1}{(2k+1)(2k+3)}$$
$$= \frac{2k^2+3k+1}{(2k+1)(2k+3)}$$
$$= \frac{(2k+1)(k+1)}{(2k+1)(2k+3)}$$
$$= \frac{k+1}{(2k+3)}$$ by algebra,

and this is the right-hand side of $P(k+1)$ *[as was to be shown]*.

32. *Hint 1:* The general formula is
$1-4+9-16+\cdots+(-1)^{n-1}n^2$
$= (-1)^{n-1}(1+2+3+\cdots+n)$ in expanded form

Or: $\displaystyle\sum_{i=1}^{n}(-1)^{i-1}i^2 = (-1)^{n-1}\left(\sum_{i=1}^{n} i\right)$ in summation notation.

Hint 2: In the proof, use the fact that
$$1+2+3+\cdots+n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

33. *Hint:*
$c+(c+d)+(c+2d)+\cdots+(c+nd)$
$= (n+1)c+d\cdot\dfrac{n(n+1)}{2}.$

36. In the inductive step, both the inductive hypothesis and what is to be shown are wrong. The inductive hypothesis should be

Suppose that for some integer $k \geq 1$,
$$1^2+2^2+\cdots+k^2 = \frac{k(k+1)(2k+1)}{6}.$$

And what is to be shown should be

$$1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

37. *Hint:* See the Caution note in Section 5.1, page 262.

38. *Hint:* See the subsection Proving an Equality on page 284 in Section 5.2.

40. *Hint:* Form the sum $n^2 + (n+1)^2 + (n+2)^2 + \cdots + (n+(p-1))^2$, and show that it equals

$$pn^2 + 2n(1+2+3+\cdots+(p-1)) + (1+4+9+16+\cdots+(p-1)^2).$$

SECTION 5.3

1. Proof: Let the property $P(n)$ be the sentence "n cents can be obtained by using 3-cent and 8-cent coins."

We will show that $P(n)$ is true for every integer $n \geq 14$.

Show that P(14) is true:

Fourteen cents can be obtained by using two 3-cent coins and one 8-cent coin.

Show that for every integer $k \geq 14$, if $P(k)$ is true then $P(k+1)$ is also true:

Suppose k is any integer with $k \geq 14$ such that k cents can be obtained using 3-cent and 8-cent coins. *[Inductive hypothesis]* We must show that $k+1$ cents can be obtained using 3-cent and 8-cent coins. If the k cents includes an 8-cent coin, replace it by three 3-cent coins to obtain a total of $k+1$ cents. Otherwise the k cents consists of 3-cent coins exclusively, and so there must be least five 3-cent coins (since the total amount is at least 14 cents). In this case, replace five of the 3-cent coins by two 8-cent coin to obtain a total of $k+1$ cents. Thus, in either case, $k+1$ cents can be obtained using 3-cent and 8-cent coins. *[This is what we needed to show.]*

[Since we have proved the basis step and the inductive step, we conclude that the given statement is true for every integer $n \geq 14$.]

4. **a.** $P(0)$ is "$5^0 - 1$ is divisible by 4." $P(0)$ is true because $5^0 - 1 = 0$, which is divisible by 4.

b. $P(k)$ is "$5^k - 1$ is divisible by 4."

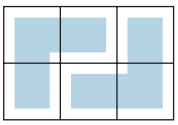
c. $P(k+1)$ is "$5^{k+1} - 1$ is divisible by 4."

d. *Must show:* If k is any integer such that $k \geq 0$ and $5^k - 1$ is divisible by 4, then $5^{k+1} - 1$ is divisible by 4.

6. For each positive integer n, let $P(n)$ be the sentence

Any checkerboard with dimensions $2 \times 3n$ can be completely covered with L-shaped trominoes.

a. $P(1)$ is the sentence "Any checkerboard with dimensions 2×3 can be completely covered with L-shaped trominoes." The following diagram shows that $P(1)$ is true:



b. $P(k)$ is the sentence "Any checkerboard with dimensions $2 \times 3k$ can be completely covered with L-shaped trominoes."

c. $P(k+1)$ is the sentence "Any checkerboard with dimensions $2 \times 3(k+1)$ can be completely covered with L-shaped trominoes."

d. The inductive step requires showing that for every integer $k \geq 1$, if any checkerboard with dimensions $2 \times 3k$ can be completely covered with L-shaped trominoes, then any checkerboard with dimensions $2 \times 3(k+1)$ can be completely covered with L-shaped trominoes.

8. Proof (by mathematical induction): For the given statement, the property is the sentence "$5^n - 1$ is divisible by 4."

Show that P(0) is true:

$P(0)$ is the sentence "$5^0 - 1$ is divisible by 4." Now $5^0 - 1 = 1 - 1 = 0$, and 0 is divisible by 4 because $0 = 4 \cdot 0$. Thus $P(0)$ is true.

Show that for every integer $k \geq 0$, if $P(k)$ is true then $P(k+1)$ is true:

Let k be any integer with $k \geq 0$, and suppose $P(k)$ is true. That is, suppose $5^k - 1$ is divisible by 4. *[This is the inductive hypothesis.]* We must show that $P(k+1)$ is true. That is, we must show that $5^{k+1} - 1$ is divisible by 4. Now

$$5^{k+1} - 1 = 5^k \cdot 5 - 1 = 5^k \cdot (4+1) - 1 = 5^k \cdot 4 + (5^k - 1). \quad (*)$$

By the inductive hypothesis, $5^k - 1$ is divisible by 4, and so $5^k - 1 = 4r$ for some integer r. Substitute $4r$ in place of $5^k - 1$ in equation (*), to obtain

$$5^{k+1} - 1 = 5^k \cdot 4 + 4r = 4(5^k + r).$$

But $5^k + r$ is an integer because k and r are integers. Hence, by definition of divisibility, $5^{k+1} - 1$ is divisible by 4 *[as was to be shown]*.

An alternative proof of the inductive step goes as follows:

Let k be any integer with $k \geq 0$, and suppose that $5^k - 1$ is divisible by 4. Then $5^k - 1 = 4r$ for some integer r, and hence $5^k = 4r + 1$.

It follows that $5^{k+1} = 5^k \cdot 5 = (4r+1) \cdot 5 = 20r + 5$. Subtracting 1 from both sides gives that $5^{k+1} - 1 = 20r + 4 = 4(5r+1)$. Now since $5r + 1$ is an integer, by definition of divisibility, $5^{k+1} - 1$ is divisible by 4.

11. Proof (by mathematical induction): For the given statement, the property $P(n)$ is the sentence "$3^{2n} - 1$ is divisible by 8."

Show that P(0) is true:

$P(0)$ is the sentence "$3^{2 \cdot 0} - 1$ is divisible by 8." Observe that $3^{2 \cdot 0} - 1 = 1 - 1 = 0$, and 0 is divisible by 8 because $0 = 8 \cdot 0$. Thus $P(0)$ is true.

Show that for every integer k ≥ 0, if P(k) is true then P(k + 1) is true:

Let k be any integer with $k \geq 0$, and suppose $P(k)$ is true. That is, suppose $3^{2k} - 1$ is divisible by 8. *[This is the inductive hypothesis.]* We must show that $P(k+1)$ is true. That is, we must show that $3^{2(k+1)} - 1$ is divisible by 8, or, equivalently, that $3^{2k+2} - 1$ is divisible by 8. Now

$$\begin{aligned} 3^{2k+2} - 1 &= 3^{2k} \cdot 3^2 - 1 = 3^{2k} \cdot 9 - 1 \\ &= 3^{2k} \cdot (8+1) - 1 = 3^{2k} \cdot 8 + (3^{2k} - 1). \end{aligned} \qquad (*)$$

By the inductive hypothesis $3^{2k} - 1$ is divisible by 8, and so $3^{2k} - 1 = 8r$ for some integer r. By substitution into equation (*),

$$3^{2k+2} - 1 = 3^{2k} \cdot 8 + 8r = 8(3^{2k} + r).$$

Now $3^{2k} + r$ is an integer because k and r are integers, and hence, by definition of divisibility, $3^{2k+2} - 1$ is divisible by 8 *[as was to be shown].*

13. *Hint:*

$$\begin{aligned} x^{k+1} - y^{k+1} &= x^{k+1} - x \cdot y^k + x \cdot y^k - y^{k+1} \\ &= x \cdot (x^k - y^k) + y^k \cdot (x - y) \end{aligned}$$

14. *Hint 1:*

$$\begin{aligned} (k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= (k^3 - k) + 3k^2 + 3k \\ &= (k^3 - k) + 3k(k+1) \end{aligned}$$

Hint 2: $k(k+1)$ is a product of two consecutive integers.

By Theorem 4.5.2, one of these must be even.

16. Proof (by mathematical induction): For the given statement, let the property $P(n)$ be the inequality $2^n < (n+1)!$.

Show that P(2) is true:

$P(2)$ says that $2^2 < (2+1)!$. The left-hand side is $2^2 = 4$ and the right-hand side is $3! = 6$. So, because $4 < 6$, $P(2)$ is true.

Show that for every integer k ≥ 2, if P(k) is true then P(k + 1) is true:

Let k be any integer with $k \geq 2$, and suppose $P(k)$ is true. That is, suppose $2^k < (k+1)!$. *[This is the inductive hypothesis.]* We must show that $P(k+1)$ is true. That is, we must show that $2^{k+1} < ((k+1)+1)$, or, equivalently, that $2^{k+1} < (k+2)!$. By the laws of exponents and the inductive hypothesis,

$$2^{k+1} = 2 \cdot 2^k < 2(k+1)!. \qquad (*)$$

Since $k \geq 2$, then $2 < k + 2$, and so

$$2(k+1)! < (k+2)(k+1)! = (k+2)!. \qquad (**)$$

Combining inequalities (*) and (**) gives

$$2^{k+1} < (k+2)!$$

[as was to be shown].

19. Proof (by mathematical induction): For the given statement, let the property $P(n)$ be the inequality $n^2 < 2^n$.

Show that P(5) is true:

$P(5)$ says that $5^2 < 2^5$. But $5^2 = 25$ and $2^5 = 32$, and $25 < 32$. Hence $P(5)$ is true.

Show that for any integer k ≥ 5, if P(k) is true then P(k + 1) is true:

Let k be any integer with $k \geq 5$, and suppose $P(k)$ is true. That is, suppose $k^2 < 2^k$. *[This is the inductive hypothesis.]* We must show that $P(k+1)$ is true. That is, we must show that $(k+1)^2 < 2^{k+1}$. Now

$$(k+1)^2 = k^2 + 2k + 1 < 2^k + 2k + 1$$

by inductive hypothesis.

Also, by Proposition 5.3.2,

$$2k + 1 < 2^k$$ Prop. 5.3.2 applies since $k \geq 5 \geq 3$.

Putting these inequalities together gives

$$(k+1)^2 < 2^k + 2k + 1 < 2^k + 2^k = 2^{k+1}$$

[as was to be shown].

24. Proof (by mathematical induction): For the given statement, let the property $P(n)$ be the equation $a_n = 3 \cdot 7^{n-1}$.

Show that P(1) is true:

The left-hand side of $P(1)$ is a_1, which equals 3 by definition of the sequence. The right-hand side is $3 \cdot 7^{1-1} = 3$ also. Thus $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is true:

Let k be any integer with $k \geq 1$, and suppose $P(k)$ is true. That is, suppose $a_k = 3 \cdot 7^{k-1}$. *[This is the inductive hypothesis.]* We must show that $P(k+1)$ is true. That is,

we must show that $a_{k+1} = 3 \cdot 7^{(k+1)-1}$, or, equivalently, $a_{k+1} = 3 \cdot 7^k$. But the left-hand side of $P(k+1)$ is

$$\begin{aligned} a_{k+1} &= 7a_k && \text{by definition of the sequence } a_1, a_2, a_3, \ldots \\ &= 7(3 \cdot 7^{k-1}) && \text{by inductive hypothesis} \\ &= 3 \cdot 7^k && \text{by the laws of exponents,} \end{aligned}$$

and this is the right-hand side of $P(k+1)$ *[as was to be shown].*

25. Proof (by mathematical induction): According to the definition of $b_0, b_1, b_2, \ldots$, we have that $b_0 = 5$ and $b_k = 4 + b_{k-1}$ for every integer $k \geq 1$. Let the property $P(n)$ be the inequality

$$b_n > 4n.$$

We will prove that $P(n)$ is true for each integer $n \geq 0$.

Show that P(0) is true: To show that $P(0)$ is true we must show that $b_0 > 4 \cdot 0$. But $4 \cdot 0 = 0$, $b_0 = 5$ (by definition of $b_0, b_1, b_2, \ldots$), and $5 > 0$. So $P(0)$ is true.

Show that for every integer k ≥ 0, if P(k) is true then P(k + 1) is true: Let k be any integer with $k \geq 0$, and suppose that

$$b_k > 4k. \quad \leftarrow \text{inductive hypothesis}$$

We must show that

$$b_{k+1} > 4(k+1).$$

Now

$$\begin{aligned} b_{k+1} &= 4 + b_k && \text{by definition of } b_0, b_1, b_2, \ldots \\ &> 4 + 4k && \text{because } b_k > 4k \text{ by inductive hypothesis} \\ &> 4(1+k) && \text{by factoring out a 4} \\ &> 4(k+1) && \text{by the commutative law of addition} \end{aligned}$$

[as was to be shown].

29. Proof (by mathematical induction):

A set L consists of strings obtained by juxtaposing one or more of *abb*, *bab*, and *bba*. Let the property $P(n)$ be the sentence "If a string s in L has length $3n$, then s contains an even number of b's."

Show that P(1) is true: $P(1)$ is the statement that a string s in L of length 3 contains an even number of b's. The only strings in L that have length 3 are *abb*, *bab*, and *bba*, and each of these strings has an even number of b's. So $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is true: Let k be any integer with $k \geq 1$ and suppose that

if a string s in L has length $3k$, then s contains an even number of b's. $\leftarrow P(k)$ inductive hypothesis

We must show that

if a string s in L has length $3(k+1)$, then s contains an even number of b's. $\leftarrow P(k+1)$

So, suppose s is a string in L that has length $3(k+1)$. Now $3(k+1) = 3k+3$ and the strings in L are obtained by juxtaposing strings already in L with one of *abb*, *bab*, or *bba*. Thus, either the initial or the final three characters in s are *abb*, *bab*, or *bba*. Moreover, the other $3k$ characters in s are also in L by definition of L, and so, by inductive hypothesis, the other $3k$ characters in s contain an even number, say m, of b's. Because each of *abb*, *bab,* and *bba* contains 2 b's, the total number of b's in s is $m+2$, which is a sum of even integers and hence is even *[as was to be shown].*

32. *Hint:* Consider the problem of trying to cover a 3×3 checkerboard with trominoes. Place a checkmark in certain squares as shown in the following figure.

✓		✓
✓		✓

Observe that no two squares containing checkmarks can be covered by the same tromino. Since there are four checkmarks, four trominoes would be needed to cover these squares. But, since each tromino covers three squares, four trominoes would cover twelve squares, not the nine squares in this checkerboard. It follows that such a covering is impossible.

34. a. *Hint:* For the inductive step, note that a $2 \times 3(k+1)$ checkerboard can be split into a $2 \times 3k$ checkerboard and a 2×3 checkerboard.

35. b. *Hint:* Consider a 3×5 checkerboard, and refer to the hint for exercise 32. Figure out a way to place six checkmarks in squares so that no two of the squares that contain checkmarks can be covered by the same tromino.

37. *Hint:* Use proof by contradiction. If the statement is false, then there exists some ordering of the integers from 1 to 30, say, $x_1, x_2, \ldots, x_{30}$, such that $x_1 + x_2 + x_3 < 45$, $x_2 + x_3 + x_4 < 45$, …, and $x_{30} + x_1 + x_2 < 45$. Evaluate the sum of all these inequalities using the fact that $\sum_{i=1}^{30} x_i = \sum_{i=1}^{30} i$ and Theorem 5.2.1.

38. *Hint:* Given $k+1$ a's and $k+1$ b's arrayed around the outside of the circle, there has to be at least one location where an a is followed by a b as one travels in the clockwise direction. In the inductive step, temporarily remove such an a and the b that follows it, and apply the inductive hypothesis.

40. b. *Hint:* In the inductive step, imagine dividing a $2(k+1) \times 2(k+1)$ checkerboard into two sections: a center checkerboard of dimensions $2k \times 2k$ and an outer perimeter of single, adjacent squares. Then examine three cases: case 1 is where both removed squares are in the central $2k \times 2k$ checkerboard, case 2 is where one removed square is in the central $2k \times 2k$ checkerboard and the other is on the perimeter, and case 3 is where both removed squares are on the perimeter.

41. *Hint:* Let $P(n)$ be the sentence: If (1) $2n+1$ people are all positioned so that the distance between any two people is different from the distance between any two other people, and if (2) each person sends a message to their nearest neighbor, then there is at least one person who does not receive a message from anyone. Use mathematical induction to prove that $P(n)$ is true for each integer $n \geq 1$.

43. a. *Hint:*

Two Balls		
WW	→	B
WB	→	W
BB	→	B

Summary			
Start		End	
W	B	W	B
2	0	0	1
1	1	1	0
0	2	0	1

b. *Hint:* In all three cases when the urn initially contains an odd number of white balls, there is one white ball in the urn at the end of the game, and when the urn initially contains an even number of white balls, there is one black ball (i.e., zero white balls) in the urn at the end of the game.

44. *Hint:* Given a graph G satisfying the given condition, form a new graph G' by deleting one vertex v of G and all the edges that are incident on v. Then apply the inductive hypothesis to G'.

45. The inductive step fails for going from $n = 1$ to $n = 2$, because when $k = 1$,

$$A = \{a_1, a_2\} \quad \text{and} \quad B = \{a_1\}$$

and no set C can be defined to have the properties claimed for the C in the proof. The reason is that $C = \{a_1\} = B$, and so an element of A, namely a_2, is not in either B or C.

Since the inductive step fails for going from $n = 1$ to $n = 2$, the truth of the following statement is never proved: "All the numbers in a set of two numbers are equal to each other." This breaks the sequence of inductive steps, and so none of the statements for $n > 2$ is proved true either.

Here is an explanation for what happens in terms of the domino analogy. The first domino *is* tipped backward (the basis step is proved). Also, if any domino from the second onward tips backward (the inductive step works or $n \geq 2$). In this case, however, when the first domino is tipped backward, it does *not* tip the second domino backward. So only the first domino falls down; the rest remain standing.

46. *Hint:* Is the basis step true?

SECTION 5.4

1. Proof (by strong mathematical induction): Let the property $P(n)$ be the sentence "a_n is odd."

Show that P(1) and P(2) are true:

Observe that $a_1 = 1$ and $a_2 = 3$ and both 1 and 3 are odd.

Thus $P(1)$ and $P(2)$ are true.

Show that for every integer $k \geq 2$, if $P(i)$ is true for each integer i with $1 \leq i \leq k$, then $P(k+1)$ is true:

Let k be any integer with $k \geq 2$, and suppose a_i is odd for each integer i with $1 \leq i \leq k$. *[This is the inductive hypothesis.]* We must show that a_{k+1} is odd. We know that $a_{k+1} = a_{k-1} + 2a_k$ by definition of $a_1, a_2, a_3, \ldots$. Moreover, $k-1$ is less than $k+1$ and is greater than or equal to 1 (because $k \geq 2$). Thus, by inductive hypothesis, a_{k-1} is odd. Also, every term of the sequence is an integer (being a sum of products of integers), and so $2a_k$ is even by definition of even. It follows that a_{k+1} is the sum of an odd integer and an even integer and hence is odd by Theorem 4.1.2 (exercise 30, Section 4.1). *[This is what was to be shown.]*

4. Proof (by strong mathematical induction): Let the property $P(n)$ be the inequality $d_n \leq 1$.

Show that P(1) and P(2) are true:

Observe that $d_1 = \frac{9}{10}$ and $d_2 = \frac{10}{11}$ and both $\frac{9}{10} \leq 1$ and $\frac{10}{11} \leq 1$. Thus $P(1)$ and $P(2)$ are true.

Show that for every integer $k \geq 2$, if $P(i)$ is true for each integer i with $1 \leq i \leq k$, then $P(k+1)$ is true:

Let k be any integer with $k \geq 2$, and suppose $d_i \leq 1$ for each integer i with $1 \leq i \leq k$. *[This is the inductive hypothesis.]* We must show that $d_{k+1} \leq 1$. Now, by definition of $d_1, d_2, d_3, \ldots, d_{k+1} = d_k \cdot d_{k-1}$. Moreover $d_k \leq 1$ and $d_{k-1} \leq 1$ by inductive hypothesis because both $k-1$ and k are less than or equal to k. Consequently, $d_{k+1} = d_k \cdot d_{k-1} \leq 1$ because if two positive numbers are each less than or equal to 1, then their product is less than or equal to 1. *[To see why this is so, note that if $0 < a \leq 1$ and $0 < b \leq 1$, then multiplying $a \leq 1$ by*

b gives ab ≤ b, and since b ≤ 1, then, by transitivity of order, ab ≤ 1.] Thus the inductive step has been proved. *[Since we have proved both the basis step and the inductive step, we conclude that $d_n \le 1$ for every integer $n \ge 1$.]*

5. Proof (by strong mathematical induction): Let the property $P(n)$ be the equation $e_n = 5 \cdot 3^n + 7 \cdot 2^n$.

Show that P(0) and P(1) are true:

We must show that $e_0 = 5 \cdot 3^0 + 7 \cdot 2^0$ and $e_1 = 5 \cdot 3^1 + 7 \cdot 2^1$. The left-hand side of the first equation is 12 (by definition of $e_0, e_1, e_2, \ldots$), and its right-hand side is $5 \cdot 1 + 7 \cdot 1 = 12$ also. The left-hand side of the second equation is 29 (by definition of $e_0, e_1, e_2, \ldots$), and its right-hand side is $5 \cdot 3 + 7 \cdot 2 = 29$ also. Thus $P(0)$ and $P(1)$ are true.

Show that for every integer k ≥ 1, if P(i) is true for each integer i with 0 ≤ i ≤ k, then P(k + 1) is true:

Let k be any integer with $k \ge 1$, and suppose $e_i = 5 \cdot 3^i + 7 \cdot 2^i$ for each integer i with $0 \le i \le k$. *[Inductive hypothesis]* We must show that $e_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$.

Now

$$\begin{aligned}
e_{k+1} &= 5e_k - 6e_{k-1} && \text{by definition of } e_0, e_1, e_2, \ldots. \\
&= 5(5 \cdot 3^k + 7 \cdot 2^k) - 6(5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}) && \text{by inductive hypothesis} \\
&= 25 \cdot 3^k + 35 \cdot 2^k - 30 \cdot 3^{k-1} - 42 \cdot 2^{k-1} \\
&= 25 \cdot 3^k + 35 \cdot 2^k - 10 \cdot 3 \cdot 3^{k-1} - 21 \cdot 2 \cdot 2^{k-1} \\
&= 25 \cdot 3^k + 35 \cdot 2^k - 10 \cdot 3^k - 21 \cdot 2^k \\
&= (25 - 10) \cdot 3^k + (35 - 21) \cdot 2^k \\
&= 15 \cdot 3^k + 14 \cdot 2^k \\
&= 5 \cdot 3 \cdot 3^k + 7 \cdot 2 \cdot 2^k \\
&= 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1} && \text{by algebra}
\end{aligned}$$

[as was to be shown].

10. *Hint:* In the basis step, show that $P(14)$, $P(15)$, and $P(16)$ are all true. For the inductive step, note that $k + 1 = [(k + 1) - 3] + 3$, and if $k \ge 16$, then $(k + 1) - 3 \ge 14$.

11. Proof (by strong mathematical induction): Let the property $P(n)$ be the sentence

> *A* jigsaw puzzle consisting of n pieces takes $n - 1$ steps to put together.

Show that P(1) is true:

A jigsaw puzzle consisting of just one piece does not take any steps to put together. Hence it is correct to say that it takes zero steps to put together.

Show that for every integer k ≥ 1, if P(i) is true for each integer i with 1 ≤ i ≤ k, then P(k + 1) is true:

Let k be any integer with $k \ge 1$ and suppose that for each integer i with $1 \le i \le k$, a jigsaw puzzle consisting of i pieces takes $i - 1$ steps to put together. *[This is the inductive hypothesis.]* We must show that a jigsaw puzzle consisting of $k + 1$ pieces takes k steps to put together. Consider assembling a jigsaw puzzle consisting of $k + 1$ pieces. The last step involves fitting together two blocks. Suppose one of the blocks consists of r pieces and the other consists of s pieces. Then $r + s = k + 1$, and $1 \le r \le k$ and $1 \le s \le k$. Thus, by the inductive hypothesis, the numbers of steps required to assemble the blocks are $r - 1$ and $s - 1$, respectively. Then the total number of steps required to assemble the puzzle is $(r - 1) + (s - 1) + 1 = (r + s) - 1 = (k + 1) - 1 = k$ *[as was to be shown].*

12. *Hint:* For any collection of cans, at least one must contain enough gasoline to enable the car to get to the next can. (Why?) Imagine taking all the gasoline from that can and pouring it into the can that immediately precedes it in the direction of travel around the track.

13. *Sketch of proof:* Given any integer $k > 1$, either k is prime or k is a product of two smaller positive integers, each greater than 1. In the former case, the property is true. In the latter case, the inductive hypothesis ensures that both factors of k are products of primes and hence that k is also a product of primes.

14. Proof (by strong mathematical induction): Let the property $P(n)$ be the sentence "Any product of n odd integers is odd."

Show that P(2) is true:

We must show that any product of two odd integers is odd. But this was established in exercise 20 of Section 4.2.

Show that for every integer k ≥ 2, if P(i) is true for each integer i with 2 ≤ i ≤ k then P(k + 1) is true:

Let k be any integer with $k \ge 2$, and suppose that for each integer i with $2 \le i \le k$, any product of i odd integers is odd. *[Inductive hypothesis]* Consider any product M of $k + 1$ odd integers. Some multiplication is the final one that is used to obtain M. Thus, there are integers A and B such that $M = AB$, and each of A and B is a product of between 1 and k odd integers. (For instance, if $M = ((a_1a_2)a_3)a_4$, then $A = (a_1a_2)a_3$ and $B = a_4$.) By inductive hypothesis, each of A and B is odd, and, as in the basis step, we know that any product of two odd integers is odd. Hence $M = AB$ is odd.

16. *Hint:* Let the property $P(n)$ be the sentence "If n is even, then any sum of n odd integers is even, and if

n is odd, then any sum of n odd integers is odd." For the inductive step, consider any sum S of $k+1$ odd integers. Some addition is the final one that is used to obtain S. Thus, there are integers A and B such that $S = A + B$, and A is a sum of r odd integers and B is a sum of $(k+1) - r$ odd integers. Consider the two cases where $k+1$ is even and $k+1$ is odd, and for each case consider the two subcases where r is even and where r is odd.

17. $4^1 = 4$, $4^2 = 16$, $4^3 = 64$, $4^4 = 256$, $4^5 = 1024$, $4^6 = 4096$, $4^7 = 16384$, and $4^8 = 65536$.

Conjecture: The units digit of 4^n equals 4 if n is odd and equals 6 if n is even.

Proof by strong mathematical induction: Let the property $P(n)$ be the sentence "The units digit of 4^n equals 4 if n is odd and equals 6 if n is even."

Show that P(1) and P(2) are true:

When $n = 1$, $4^n = 4^1 = 4$, and so the units digit is 4. When $n = 2$, then $4^n = 4^2 = 16$, and so the units digit is 6. Thus, $P(1)$ and $P(2)$ are true.

Show that for every integer $k \geq 2$, if the property is true for each integer i with $1 \leq i \leq k$ then it is true for $k+1$:

Let k by any integer with $k \geq 2$, and suppose that for each integer i with $0 \leq i \leq k$, the units digit of 4^i equals 4 if i is odd and equals 6 if i is even. *[Inductive hypothesis]* We must show that the units digit of 4^{k+1} equals 4 if $k+1$ is odd and equals 6 if $k+1$ is even.

Case 1 ($k+1$ is odd): In this case, k is even, and so, by inductive hypothesis, the units digits of 4^k is 6. Thus $4^k = 10q + 6$ for some nonnegative integer q. It follows that $4^{k+1} = 4^k \cdot 4 = (10q+6)\cdot 4 = 40q + 24 = 10(4q+2) + 4$. Thus, the units digit of 4^{k+1} is 4.

Case 2 ($k+1$ is even): In this case, k is odd, and so, by inductive hypothesis, the units digit of 4^k is 4. Thus $4^k = 10q + 4$ for some nonnegative integer q. It follows that $4^{k+1} = 4^k \cdot 4 = (10q+4)\cdot 4 = 40q + 16 = 10(4q+1) + 6$. Thus, the units digit of 4^{k+1} is 6.

Conclusion: Because cases 1 and 2 are the only possibilities and 4^{k+1} has one of the required forms in each case, we have shown that $P(k+1)$ is true.

19. Proof (by strong mathematical induction): Let a_1, a_2, a_3, … be a sequence that satisfies the recurrence relation $a_k = 2 \cdot a_{\lfloor k/2 \rfloor}$ for every integer $k \geq 2$, with initial condition $a_1 = 1$, and let the property $P(n)$ be the inequality

$$a_n \leq n. \qquad \leftarrow P(n)$$

We will show that $P(n)$ is true for each integer $n \geq 1$.

Show that P(1) is true: $a_1 = 1$ and $1 \leq 1$. So $P(1)$ is true.

Show that for every integer $k \geq 1$, if $P(i)$ is true for each integer i from 1 through k, then $P(k+1)$ is true: Let k be any integer with $k \geq 1$, and suppose that

$a_i \leq i$ for each integer i with $1 \leq i \leq k$. ← inductive hypothesis

We must show that

$$a_{k+1} \leq k+1.$$

Now

$$\begin{aligned} a_{k+1} &= 2 \cdot a_{\lfloor (k+1)/2 \rfloor} && \text{by definition of } a_1, a_2, a_3, \ldots \\ &\leq 2 \cdot \lfloor (k+1)/2 \rfloor \\ &\leq \begin{cases} 2 \cdot ((k+1)/2) & \text{if } k \text{ is odd} \\ 2 \cdot (k/2) & \text{if } k \text{ is even} \end{cases} && \text{by inductive hypothesis} \\ &\leq \begin{cases} k+1 & \text{if } k \text{ is odd} \\ k & \text{if } k \text{ is even} \end{cases} \\ &\leq k+1 && \text{because both } k \leq k+1 \text{ and } k+1 \leq k+1. \end{aligned}$$

Thus $a_{k+1} \leq k+1$ *[as was to be shown].*

22. Proof (by strong mathematical induction): Let $P(n)$ be the sentence

> In this version of NIM, if both piles initially contain n objects, the player who goes second can always win.

We will prove that $P(n)$ is true for every integer $n \geq 0$.

Show that P(0) is true:

If neither pile contains any objects, the player who goes first automatically loses because of not being able to make a move. So the second player wins the game by default. Thus $P(0)$ is true.

Show that for every integer $k \geq 0$, if $P(i)$ is true for each integer i from 1 through k, then $P(k+1)$ is true:

Let k be any integer with $k \geq 0$, and suppose:

> In this version of NIM, for every integer i with $0 \leq i \leq k$, if both piles initially contain i objects, the player who goes second can always win.

We must show that

> In this version of NIM, if both piles initially contain $k+1$ objects, the player who goes second can always win. ← $P(k+1)$

So suppose both piles contain $k + 1$ objects, where $0 \le i \le k$, and suppose the first player removes r objects from pile #1, where $1 \le r \le 3$. If the second player removes r objects from pile #2, then both piles will have the same number of objects, namely $(k+1) - r$ and $(k+1) - r \le k$ because $r \ge 1$. Thus, by inductive hypothesis, the second player can win.

23. a.

<table>
<tr><td colspan="10">10</td><td></td><td></td></tr>
<tr><td colspan="3">3</td><td colspan="7">7</td><td>3 · 7</td><td>21</td></tr>
<tr><td>1</td><td colspan="2">2</td><td colspan="4">4</td><td colspan="3">3</td><td>1 · 2 + 4 · 3</td><td>14</td></tr>
<tr><td></td><td>1</td><td>1</td><td colspan="2">2</td><td colspan="2">2</td><td>1</td><td colspan="2">2</td><td>1 · 1 + 2 · 2 + 1 · 2</td><td>7</td></tr>
<tr><td colspan="3"></td><td>1</td><td>1</td><td>1</td><td>1</td><td></td><td>1</td><td>1</td><td>1 · 1 + 1 · 1 + 1 · 1</td><td>3</td></tr>
<tr><td colspan="10"></td><td>TOTAL</td><td>45</td></tr>
</table>

24. a. The results are shown both diagrammatically and in a table.

Round	Eliminated	Remaining
1	2, 4, 6, 8, 10, 12, 14, 16	1, 3, 5, 7, 9, 11, 13
2	3, 7, 11, 15	1, 5, 9, 13
3	5, 13	1, 9
4	9	1

26. Proof: Let n be any integer greater than 1. Consider the set S of all positive integers other than 1 that divide n. Since $n \mid n$ and $n > 1$, there is at least one element in S. Hence, by the well-ordering principle for the integers, S has a smallest element; call it p. We claim that p is prime. For suppose p is not prime. Then there are integers a and b with $1 < a < p$, $1 < b < p$, and $p = ab$. By definition of divides, $a \mid p$. Also $p \mid n$ because p is in S and every element in S divides n. Therefore, $a \mid p$ and $p \mid n$, and so, by transitivity of divisibility, $a \mid n$. Consequently, $a \in S$. But this contradicts the fact that $a < p$, and p is the smallest element of S. *[This contradiction shows that the supposition that p is not prime is false.]* Hence p is prime, and we have shown the existence of a prime number that divides n.

28. a. Proof: Suppose r is any rational number. *[We need to show that there is an integer n such that $r < n$.]*

***Case 1* ($r \le 0$):** In this case, take $n = 1$. Then $r < n$.

***Case 2* ($r > 0$):** In this case, $r = \frac{a}{b}$ for some positive integers a and b (by definition of rational and because r is positive). Note that $r = \frac{a}{b} < n$ if, and only if, $a < nb$. Let $n = 2a$. Multiply both sides of the inequality $1 < 2$ by a to obtain $a < 2a$, and multiply both sides of the inequality $1 < b$ by $2a$ to obtain $2a < 2ab = nb$. Thus $a < 2a < nb$, and so, by transitivity of order, $a < nb$. Dividing both sides by b gives that $\frac{a}{b} < n$, or, equivalently, that $r < n$.

Hence, in both cases, $r < n$ *[as was to be shown]*.

29. *Hint:* If r is any rational number, let S be the set of all integers n such that $r < n$. Use the results of exercises 28(a), 28(c), and the well-ordering principle for the integers to show that S has a least element, say v, and then show that $v - 1 \le r < v$.

30. Proof: Let S be the set of all integers r such that $n = 2^i \cdot r$ for some integer i. Then $n \in S$ because $n = 2^0 \cdot n$, and so $S \ne \varnothing$. Also, since $n \ge 1$, each r in S is positive, and so, by the well-ordering principle, S has a least element m. This means that $n = 2^k \cdot m$ (*) for some nonnegative integer k, and $m \le r$ for every r in S. We claim that m is odd. The reason is that if m is even, then $m = 2p$ for some integer p. Substituting into equation (*) gives

$$n = 2^k \cdot m = 2^k \cdot 2p = (2^k \cdot 2)p = 2^{k+1} \cdot p.$$

It follows that $p \in S$ and $p < m$, which contradicts the fact that m is the *least* element of S. Hence m is odd, and so $n = m \cdot 2^k$ for some odd integer m and nonnegative integer k.

34. *Hint:* In the inductive step, divide into cases depending on whether k can be written as $k = 3x$ or $k = 3x + 1$ or $k = 3x + 2$ for some integer x.

35. *Hint:* In the inductive step, let an integer $k \ge 0$ be given and suppose that there exist integers q' and r' such that $k = dq' + r'$ and $0 \le r' < d$. You must show that there exist integers q and r such that

$$k + 1 = dq + r \text{ and } 0 \le r < d.$$

To do this, consider the two cases $r' < d - 1$ and $r' = d - 1$.

36. *Hint:* Given a predicate $P(n)$ that satisfies conditions (1) and (2) of the principle of mathematical induction, let S be the set of all integers greater than or equal to a

for which $P(n)$ is false. Suppose that S has one or more elements, and use the well-ordering principle for the integers to derive a contradiction.

37. *Hint:* Suppose S is a set containing one or more integers, all of which are greater than or equal to some integer a, and suppose that S does not have a least element. Let the property $P(n)$ be the sentence "$i \notin S$ for any integer i with $a \le i \le n$." Use mathematical induction to prove that $P(n)$ is true for every integer $n \ge a$, and explain how this result contradicts the supposition that S does not have a least element.

SECTION 5.5

1. Proof: Suppose the predicate $m + n = 100$ is true before entry to the loop. Then

$$m_{\text{old}} + n_{\text{old}} = 100.$$

After execution of the loop,

$$m_{\text{new}} = m_{\text{old}} + 1 \text{ and } n_{\text{new}} = n_{\text{old}} - 1,$$

so

$$\begin{aligned} m_{\text{new}} + n_{\text{new}} &= (m_{\text{old}} + 1) + (n_{\text{old}} - 1) \\ &= m_{\text{old}} + n_{\text{old}} = 100. \end{aligned}$$

3. Proof: Suppose the predicate $m^3 > n^2$ is true before entry to the loop. Then

$$m_{\text{old}}^3 > n_{\text{old}}^2.$$

After execution of the loop,

$$m_{\text{new}} = 3 \cdot m_{\text{old}} \quad \text{and} \quad n_{\text{new}} = 5 \cdot n_{\text{old}},$$

so

$$m_{\text{new}}^3 = (3 \cdot m_{\text{old}})^3 = 27 \cdot m_{\text{old}}^3 > 27 \cdot n_{\text{old}}^2.$$

Now since $n_{\text{new}} = 5 \cdot n_{\text{old}}$, then $n_{\text{old}} = \frac{1}{5} n_{\text{new}}$. Hence

$$\begin{aligned} m_{\text{new}}^3 > 27 \cdot n_{\text{old}}^2 &= 27 \cdot \left(\frac{1}{5} n_{\text{new}}\right)^2 = 27 \cdot \frac{1}{25} n_{\text{new}}^2 \\ &= \frac{27}{25} \cdot n_{\text{new}}^2 > n_{\text{new}}^2. \end{aligned}$$

6. Proof: *[The wording of this proof is almost the same as that of Example 5.5.2.]*

I. Basis Property: *[$I(0)$ is true before the first iteration of the loop.]*

$I(0)$ is "$exp = x^0$ and $i = 0$." According to the pre-condition, before the first iteration of the loop $exp = 1$ and $i = 0$. Since $x^0 = 1$, $I(0)$ is evidently true.

II. Inductive Property: *[If $G \wedge I(k)$ is true before a loop iteration (where $k \ge 0$), then $(k + 1)$ is true after the loop iteration.]*

Suppose k is any nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then as execution reaches the top of the loop, $i \ne m$, $exp = x^k$, and $i = k$. Since $i \ne m$, the guard is passed and statement 1 is executed. Now before execution of statement 1,

$$exp_{\text{old}} = x^k,$$

so execution of statement 1 has the following effect:

$$exp_{\text{new}} = exp_{\text{old}} \cdot x = x^k \cdot x = x^{k+1}.$$

Similarly, before statement 2 is executed,

$$i_{\text{old}} = k,$$

so after execution of statement 2,

$$i_{\text{new}} = i_{\text{old}} + 1 = k + 1$$

Hence after the loop iteration, the two statements $exp = x_{k+1}$ and $i = k + 1$ are true, and so $I(k + 1)$ is true.

III. Eventual Falsity of Guard: *[After a finite number of iterations of the loop, G becomes false.]*

The guard G is the condition $i \ne m$, and m is a nonnegative integer. By I and II, it is known that

> for every integer $n \ge 0$, if the loop is iterated n times, then $exp = x^n$ and $i = n$.

So after m iterations of the loop, $i = m$. Thus G becomes false after m iterations of the loop.

IV. Correctness of the Post-Condition: *[If N is the least number of iterations after which G is false and I(N) is true, then the value of the algorithm variables will be as specified in the post-condition of the loop.]*

According to the post-condition, the value of exp after execution of the loop should be x^m. But when G is false, $i = m$. And when $I(N)$ is true, $i = N$ and $exp = x^N$. Since *both* conditions (G false and $I(N)$ true) are satisfied, $m = i = N$ and $exp = x^m$, as required.

8. Proof:

I. Basis Property: $I(0)$ is "$i = 1$ and $sum = A[1]$." According to the pre-condition, this statement is true.

II. Inductive Property: Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then as execution reaches the top of the loop, $i \ne m$, $i = k + 1$, and $sum = A[1] + A[2] + \cdots + A[k + 1]$. Since $i \ne m$, the guard is passed and statement 1 is executed. Now before execution of statement 1, $i_{\text{old}} = k + 1$. So after execution of statement 1, $i_{\text{new}} = i_{\text{old}} + 1 = (k + 1) + 1 = k + 2$. Also before statement 2 is executed, $sum_{\text{old}} = A[1] + A[2] + \cdots + A[k + 1]$.

Execution of statement 2 adds $A[k+2]$ to this sum, and so after statement 2 is executed, $sum_{new} = A[1] + A[2] + \cdots + A[k+1] + A[k+2]$. Thus after the loop iteration, $I(k+1)$ is true.

III. Eventual Falsity of Guard: The guard G is the condition $i \neq m$. By I and II, it is known that for every integer $n \geq 1$, after n iterations of the loop, $I(n)$ is true. Hence, after $m-1$ iterations of the loop, $I(m)$ is true, which implies that $i = m$ and G is false.

IV. Correctness of the Post-Condition: Suppose that N is the least number of iterations after which G is false and $I(N)$ is true. Then (since G is false) $i = m$ and (since $I(N)$ is true) $i = N+1$ and $sum = A[1] + A[2] + \cdots + A[N+1]$. Putting these together gives $m = N+1$, and so $sum = A[1] + A[2] + \cdots + A[m]$, which is the post-condition.

10. *Hint:* Assume $G \wedge I(k)$ is true for a nonnegative integer k. Then $a_{\text{old}} \neq 0$ and $b_{\text{old}} \neq 0$ and

(1) a_{old} and b_{old} are nonnegative integers with $\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(A, B)$.
(2) At most one of a_{old} and b_{old} equals 0.
(3) $0 \leq a_{\text{old}} + b_{\text{old}} \leq A + B - k$.

It must be shown that $I(k+1)$ is true after the loop iteration. That means it is necessary to show that

(1) a_{new} and b_{new} are nonnegative integers with $\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(A, B)$.
(2) At most one of a_{new} and b_{new} equals 0.
(3) $0 \leq a_{\text{new}} + b_{\text{new}} \leq A + B - (k+1)$.

To show (3), observe that

$$a_{\text{new}} + b_{\text{new}} = \begin{cases} a_{\text{old}} - b_{\text{old}} + b_{\text{old}} & \text{if } a_{\text{old}} \geq b_{\text{old}} \\ b_{\text{old}} - a_{\text{old}} + a_{\text{old}} & \text{if } a_{\text{old}} < b_{\text{old}} \end{cases}.$$

[The reason for this is that when $a_{old} \geq b_{old}$, then $a_{new} = a_{old} - b_{old}$ and $b_{new} = b_{old}$, and when $a_{old} < b_{old}$, then $b_{new} = b_{old} - a_{old}$ and $a_{new} = a_{old}$.]

$$a_{\text{new}} + b_{\text{new}} = \begin{cases} a_{\text{old}} & \text{if } a_{\text{old}} \geq b_{\text{old}} \\ b_{\text{old}} & \text{if } a_{\text{old}} < b_{\text{old}} \end{cases}.$$

Now since $a_{\text{old}} \neq 0$ and $b_{\text{old}} \neq 0$, and since a_{old} and b_{old} are nonnegative integers, then $a_{\text{old}} \geq 1$ and $b_{\text{old}} \geq 1$. Hence, $a_{\text{old}} - 1 \geq 0$ and $b_{\text{old}} - 1 \geq 0$, and so $a_{\text{old}} \leq a_{\text{old}} + b_{\text{old}} - 1$ and $b_{\text{old}} \leq b_{\text{old}} + a_{\text{old}} - 1$. It follows that $a_{\text{new}} + a_{\text{new}} \leq a_{\text{old}} + b_{\text{old}} - 1 \leq (A + B - k) - 1$ by noting that (3) is true when going into the kth iteration. Thus, $a_{\text{new}} + b_{\text{new}} < A + B - (k+1)$ by algebraic simplification.

SECTION 5.6

1. $a_1 = 1$, $a_2 = 2a_1 + 2 = 2 \cdot 1 + 2 = 4$,
$a_3 = 2a_2 + 3 = 2 \cdot 4 + 3 = 11$,
$a_4 = 2a_3 + 4 = 2 \cdot 11 + 4 = 26$

3. $c_0 = 1$, $c_1 = 1 \cdot (c_0)^2 = 1 \cdot (1)^2 = 1$,
$c_2 = 2(c_1)^2 = 2 \cdot (1)^2 = 2$,
$c_3 = 3(c_2)^2 = 3 \cdot (2)^2 = 12$

5. $s_0 = 1$, $s_1 = 1$, $s_2 = s_1 + 2s_0 = 1 + 2 \cdot 1 = 3$,
$s_3 = s_2 + 2s_1 = 3 + 2 \cdot 1 = 5$

7. $u_1 = 1$, $u_2 = 1$, $u_3 = 3u_2 - u_1 = 3 \cdot 1 - 1 = 2$,
$u_4 = 4u_3 - u_2 = 4 \cdot 2 - 1 = 7$

9. By definition of $a_0, a_1, a_2, \ldots$, for each integer $k \geq 1$,

(*) $a_k = 3k + 1$ and
(**) $a_{k-1} = 3(k-1) + 1$.

Then $a_{k-1} + 3$

$= 3(k-1) + 1 + 3$ by substitution from (**)
$= 3k - 3 + 1 + 3$
$= 3k + 1$ by basic algebra
$= a_k$ by substitution from (*).

11. By definition of $c_0, c_1, c_2, \ldots, c_n = 2^n - 1$, for each integer $n \geq 0$. Substitute k and $k-1$ in place of n to get

(*) $c_k = 2^k - 1$ and
(**) $c_{k-1} = 2^{k-1} - 1$

for every integer $k \geq 1$. Then

$2c_{k-1} + 1 = 2(2^{k-1} - 1) + 1$ by substitution from (**)
$= 2^k - 2 + 1$
$= 2^k - 1$ by basic algebra
$= c_k$ by substitution from (*).

13. By definition of $t_0, t_1, t_2, \ldots, t_n = 2 + n$, for each integer $n \geq 0$. Substitute k, $k-1$, and $k-2$ in place of n to get

(*) $t_k = 2 + k$,
(**) $t_{k-1} = 2 + (k-1)$, and
(***) $t_{k-2} = 2 + (k-2)$

for each integer $k \geq 2$. Then

$2t_{k-1} - t_{k-2}$
$= 2(2 + (k-1)) - (2 + (k-2))$ by substitution from (**) and (***)
$= 2(k+1) - k$
$= 2 + k$ by basic algebra
$= t_k$ by substitution from (*).

15. *Hint:* Mathematical induction is not needed for the proof. Start with the right-hand side of the equation and

use algebra to transform it into the left-hand side of the equation.

17. a. $a_1 = 2$

$a_2 = 2$ (moves to move the top disk from pole A to pole C)
$+ 1$ (move to move the bottom disk from pole A to pole B)
$+ 2$ (moves to move top disk from pole C to pole A)
$+ 1$ (move to move the bottom disk from pole B to pole C)
$+ 2$ (moves to move top disk from pole A to pole C)
$= 8$

$a_3 = 8 + 1 + 8 + 1 + 8 = 26$

c. For every integer $k \geq 2$,

$a_k = a_{k-1}$ (moves to move the top $k-1$ disks from pole A to pole C)
$+ 1$ (move to move the bottom disk from pole A to pole B)
$+ a_{k-1}$ (moves to move the top disk from pole C to pole A)
$+ 1$ (move to move the bottom disks from pole B to pole C)
$+ a_{k-1}$ (moves to move the top disks from pole A to pole C)
$= 3a_{k-1} + 2.$

18. b. $b_4 = 40$

e. *Hint:* One solution is to use mathematical induction and apply the formula from part (c). Another solution is to prove by mathematical induction that when a most efficient transfer of n disks from one end pole to the other end pole is performed, at some point all the disks are on the middle pole.

19. a. $s_1 = 1, s_2 = 1 + 1 + 1 = 3,$

$s_3 = s_1 + (1 + 1 + 1) + s_1 = 5$

b. $s_4 = s_2 + (1 + 1 + 1) + s_2 = 9$

20. b. Call the poles A, B, and C. Compute c_2 by using the following sequence of steps to transfer two disks from A to B:

1 (move to transfer the top disk from A to B)
$+ 1$ (move to transfer the top disk from B to C)
$+ 1$ (move to transfer the bottom disk from A to B)
$+ 1$ (move to transfer the top disk from C to A)
$+ 1$ (move to transfer the top disk from A to B).

This sequence of steps is the least possible, and so $c_2 = 5$.

A tower of 3 disks can be transferred from A to B by using the following sequence of steps:

1 (move to transfer the top disk from A to B)
$+ 1$ (move to transfer the top disk from B to C)
$+ 1$ (move to transfer the middle disk from A to B)
$+ 1$ (move to transfer the top disk from C to A)
$+ 1$ (move to transfer the middle disk from B to C)
$+ 1$ (move to transfer the top disk from A to B)
$+ 1$ (move to transfer the top disk from B to C).

After these 7 steps have been completed, the bottom disk can be transferred from A to B. At that point the top two disks are on C, and a modified version of the initial seven steps can be used to transfer them from C to B. Thus the total number of steps is $7 + 1 + 7 = 15$, and $15 < 21 = 4c_2 + 1$.

21. b. $t_3 = 14$

22. b. $r_0 = 1, r_1 = 1, r_2 = 1 + 4 \cdot 1 = 5, r_3 = 5 + 4 \cdot 1 = 9,$
$r_4 = 9 + 4 \cdot 5 = 29, r_5 = 29 + 4 \cdot 9 = 65,$
$r_6 = 65 + 4 \cdot 29 = 181$

23. c. There are 904 rabbit pairs, or 1,808 rabbits, after 12 months.

25. a. Each term of the Fibonacci sequence beyond the second equals the sum of the previous two. For any integer $k \geq 1$, the two terms previous to F_{k+1} are F_k and F_{k-1}. Hence, for every integer $k \geq 1$, $F_{k+1} = F_k + F_{k-1}$.

26. By repeated use of definition of the Fibonacci sequence, for each integer $k \geq 4$,

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} = (F_{k-2} + F_{k-3}) + (F_{k-3} + F_{k-4}) \\ &= ((F_{k-3} + F_{k-4}) + F_{k-3}) + (F_{k-3} + F_{k-4}) \\ &= 3F_{k-3} + 2 + F_{k-4}. \end{aligned}$$

27. For each integer $k \geq 1$,

$$\begin{aligned} & F_k^2 - F_{k-1}^2 \\ &= (F_k - F_{k-1})(F_k + F_{k-1}) && \text{by basic algebra (difference of two squares)} \\ &= (F_k - F_{k-1})F_{k+1} && \text{by definition of the Fibonacci sequence.} \\ &= F_k F_{k+1} - F_{k-1}F_{k+1} \end{aligned}$$

32. *Hint:* Use mathematical induction. In the inductive step, use Lemma 4.10.2 and the fact that $F_{k+2} = F_{k+1} + F_k$ to deduce that

$$\gcd(F_{k+2}, F_{k+1}) = \gcd(F_{k+1}, F_k).$$

34. *Hint:* Let $L = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}$ and show that $L = \frac{1}{L} + 1$.

Deduce that $L = \frac{1+\sqrt{5}}{2}$.

35. *Hint:* Use the result of exercise 30 to prove that the infinite sequence $\frac{F_0}{F_1}, \frac{F_2}{F_3}, \frac{F_4}{F_5}, \ldots$ is strictly decreasing and that the infinite sequence $\frac{F_1}{F_2}, \frac{F_3}{F_4}, \frac{F_5}{F_6}, \ldots$ is strictly increasing. The first sequence is bounded below by 0, and the second sequence is bounded above by 1. Deduce that the limits of both sequences exist, and show that they are equal.

37. **a.** Because the 4% annual interest is compounded quarterly, the quarterly interest rate is $(4\%)/4 = 1\%$. Then $R_k = R_{k-1} + 0.01R_{k-1} = 1.01R_{k-1}$.

b. Because one year equals four quarters, the amount on deposit at the end of one year is $R_4 = \$5{,}203.02$ (rounded to the nearest cent).

c. The annual percentage yield (APY) for the account is $\frac{\$5203.02 - \$5000.00}{\$5000.00} = 4.0604\%$.

39. When one is climbing a staircase consisting of n stairs, the last step taken is either a single stair or two stairs together. The number of ways to climb the staircase and have the final step be a single stair is c_{n-1}; the number of ways to climb the staircase and have the final step be two stairs is c_{n-2}. Therefore, $c_n = c_{n-1} + c_{n-2}$. Note also that $c_1 = 1$ and $c_2 = 2$ *[because either the two stairs can be climbed one by one or they can be climbed as a unit].*

41. Proof (by mathematical induction): Let the property, $P(n)$, be the equation $\sum_{i=1}^{n} ca_i = \sum_{i=1}^{n} a_i$, where a_1, a_2, a_3, …, a_n and c are any real numbers.

Show that P(1) is true:

Let a_1 and c be any real numbers. By the recursive definition of sum, $\sum_{i=1}^{1}(ca_i) = ca_1$ and $\sum_{i=1}^{1} a_i = a_1$. Therefore, $\sum_{i=1}^{1}(ca_i) = c\sum_{i=1}^{1} a_i$, and so $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

Let k be any integer with $k \geq 1$. Suppose that for any real numbers $a_1, a_2, a_3, \ldots, a_k$ and c, $\sum_{i=1}^{k}(ca_i) = c\sum_{i=1}^{k} a_i$. *[This is the inductive hypothesis.] [We must show that for any real numbers $a_1, a_2, a_3, \ldots, a_{k+1}$ and c, $\sum_{i=1}^{k+1}(ca_i) = c\sum_{i=1}^{k+1} a_i$.]*

Let $a_1, a_2, a_3, \ldots, a_{k+1}$ and c be any real numbers. Then

$$\sum_{i=1}^{k+1} ca_i = \sum_{i=1}^{k} ca_i + ca_{k+1} \quad \text{by the recursive definition of } \Sigma$$

$$= c\sum_{i=1}^{k} a_i + ca_{k+1} \quad \text{by inductive hypothesis}$$

$$= c\left(\sum_{i=1}^{k} a_i + a_{k+1}\right) \quad \text{by the distributive law for the real numbers}$$

$$= c\sum_{i=1}^{k+1} a_i \quad \text{by the recursive definition of } \Sigma.$$

44. *Hint:* Let the property be the inequality

$$\left|\sum_{i=1}^{n} a_i\right| \leq \sum_{i=1}^{n} |a_i|.$$

To prove the inductive step, note that because $\left|\sum_{i=1}^{k+1} a_i\right| = \left|\sum_{i=1}^{k} a_i + a_{k+1}\right|$, you can use the triangle inequality for absolute value (Theorem 4.5.6) to deduce

$$\left|\sum_{i=1}^{k} a_i + a_{k+1}\right| \leq \left|\sum_{i=1}^{k} a_i\right| + |a_{k+1}|.$$

45. We give two proofs for the given statement, one less formal and the other more formal.

Proof 1 (by mathematical induction): For the basis step observe that any "sum" of one even integer is the integer itself, which is even. For the inductive step we suppose that for an arbitrarily chosen even integer $r \geq 1$., the sum of any r even integers is even. Then we must show that any sum of $r + 1$ even integers is even. But any sum of $r + 1$ even integers is equal to a sum of r even integers, which is even (by inductive hypothesis), plus another even integer. The result is a sum of two even integers, which is even (by Theorem 4.1.1) *[as was to be shown].*

Proof 2 (by mathematical induction): Let $P(n)$ be the sentence:

> If $a_1, a_2, a_3, \ldots, a_n$ are any even integers, then $\sum_{i=1}^{n} a_i$ is even. ← $P(n)$

We will show that $P(n)$ is true for every integer $n \geq 1$.

Show that P(n) is true for n = 1:

Suppose a_1 is any even integer. Then $\sum_{i=1}^{1} a_i = a_1$, which is even. So $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

Let k be any integer with $k \geq 1$, and suppose that

> If $a_1, a_2, a_3, \ldots, a_k$ are any even integers, then $\sum_{i=1}^{k} a_i$ is even. ← $P(k)$ inductive hypothesis

We must show that

> If $a_1, a_2, a_3, \ldots, a_{k+1}$ are any even integers, then $\sum_{i=1}^{k+1} a_i$ is even. ← $P(k+1)$

So suppose $a_1, a_2, a_3, \ldots, a_{k+1}$ are any even integers, then

$$\sum_{i=1}^{k+1} a_i = \sum_{i=1}^{k} a_i + a_{k+1}$$

by writing the final term of the sum separately. Now, by inductive hypothesis, $\sum_{i=1}^{k} a_i$ is even, and, by assumption, a_{k+1} is even. Therefore, $\sum_{i=1}^{k+1} a_i$ is the sum of two even integers, which is even (by Theorem 4.1.1) *[as was to be shown]*.

47. *Hint:* Use proof by contradiction or proof by contraposition.

SECTION 5.7

1. a. $1 + 2 + 3 + \cdots + (k-1)$
$$= \frac{(k-1)((k-1)+1)}{2} = \frac{(k-1)k}{2}$$

b. $5 + 2 + 4 + 6 + 8 + \cdots + 2n$
$$= 5 + 2(1 + 2 + 3 + \cdots + n)$$
$$= 5 + 2\frac{n(n+1)}{2} = 5 + n(n+1)$$
$$= n^2 + n + 5$$

2. a. $1 + 2 + 2^2 + \cdots + 2^{i-1} = \dfrac{2^{(i-1)+1} - 1}{2-1} = 2^i - 1$

c. $2^n + 2^{n-2}\cdot 3 + 2^{n-3}\cdot 3 + \cdots + 2^2\cdot 3 + 2\cdot 3 + 3$
$$= 2^n + 3(2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2 + 1)$$
$$= 2^n + 3(1 + 2 + 2^2 + \cdots + 2^{n-3} + 2^{n-2})$$
$$= 2^n + 3\left(\frac{2^{(n-2)+1} - 1}{2-1}\right)$$
$$= 2^n + 3(2^{n-1} - 1)$$
$$= 2\cdot 2^{n-1} + 3\cdot 2^{n-1} - 3$$
$$= 5\cdot 2^{n-1} - 3$$

3. $a_0 = 1$
$a_1 = 1\cdot a_0 = 1\cdot 1 = 1$
$a_2 = 2a_1 = 2\cdot 1$
$a_3 = 3a_2 = 3\cdot 2\cdot 1$
$a_4 = 4a_3 = 4\cdot 3\cdot 2\cdot 1$
$\vdots$
Guess:
$a_n = n(n-1)\cdots 3\cdot 2\cdot 1 = n!$

5. $c_1 = 1$
$c_2 = 3c_1 + 1 = 3\cdot 1 + 1 = 3 + 1$
$c_3 = 3c_2 + 1 = 3\cdot(3+1) + 1 = 3^2 + 3 + 1$
$c_4 = 3c_3 + 1 = 3\cdot(3^2 + 3 + 1) + 1$
$= 3^3 + 3^2 + 3 + 1$
$\vdots$
Guess:
$c_n = 3^{n-1} + 3^{n-2} + \cdots + 3^3 + 3^2 + 3 + 1$
$= \dfrac{3^n - 1}{3-1}$ by Theorem 5.2.2 with $r = 3$
$= \dfrac{3^n - 1}{2}$

6. *Hint:*
$d_n = 2^n + 2^{n-2}\cdot 3 + 2^{n-3}\cdot 3 + \cdots + 2^2\cdot 3 + 2\cdot 3 + 3$
$= 5\cdot 2^{n-1} - 3$
for every integer $n \geq 1$.

9. *Hint:* For any positive real numbers a and b,

$$\frac{\frac{a}{b}}{\frac{a}{b}+2} = \frac{\frac{a}{b}}{\frac{a}{b}+2}\cdot\frac{b}{b} = \frac{a}{a+2b}.$$

10. $h_0 = 1$
$h_1 = 2^1 - h_0 = 2^1 - 1$
$h_2 = 2^2 - h_1 = 2^2 - (2^1 - 1) = 2^2 - 2^1 + 1$
$h_3 = 2^3 - h_2 = 2^3 - (2^2 - 2^1 + 1)$
$= 2^3 - 2^2 + 2^1 - 1$
$h_4 = 2^4 - h_3 = 2^4 - (2^3 - 2^2 + 2^2 - 1)$
$= 2^4 - 2^3 + 2^2 - 2^1 + 1$
$\vdots$
Guess:
$h_n = 2^n - 2^{n-1} + \cdots + (-1)^n\cdot 1$
$= (-1)^n[1 - 2 + 2^2 - \cdots + (-1)^n\cdot 2^n]$
$= (-1)^n[1 + (-2) + (-2)^2 - \cdots + (-2)^n]$ by basic algebra
$= (-1)^n\left[\dfrac{(-2)^{n+1} - 1}{(-2) - 1}\right]$ by Theorem 5.2.2
$= \dfrac{(-1)^{n+1}\cdot[(-2)^{n+1} - 1]}{(-1)\cdot(-3)}$
$= \dfrac{2^{n+1} - (-1)^{n+1}}{3}$ by basic algebra

12. $s_0 = 3$

$s_1 = s_0 + 2\cdot 1 = 3 + 2\cdot 1$

$s_2 = s_1 + 2\cdot 2 = [3 + 2\cdot 1] + 2\cdot 2$
$= 3 + 2\cdot(1 + 2)$

$s_3 = s_2 + 2\cdot 3 = [3 + 2\cdot(1 + 2)] + 2\cdot 3$
$= 3 + 2\cdot(1 + 2 + 3)$

$s_4 = s_3 + 2\cdot 4 = [3 + 2\cdot(1 + 2 + 3)] + 2\cdot 4$
$= 3 + 2\cdot(1 + 2 + 3 + 4)$

$\vdots$

Guess:

$s_n = 3 + 2\cdot(1 + 2 + 3 + \cdots + (n-1) + n)$
$= 3 + 2\cdot\dfrac{n(n+1)}{2}$ by Theorem 5.2.1
$= 3 + n(n+1)$ by basic algebra

14. $x_1 = 1$

$x_2 = 3x_1 + 2 = 3 + 2$

$x_3 = 3x_2 + 3 = 3(3 + 2) + 3 = 3^2 + 3\cdot 2 + 3$

$x_4 = 3x_3 + 4 = 3(3^2 + 3\cdot 2 + 3) + 4$
$= 3^3 + 3^2\cdot 2 + 3\cdot 3 + 4$

$x_5 = 3x_4 + 5 = 3(3^3 + 3^2\cdot 2 + 3\cdot 3 + 4) + 5$
$= 3^4 + 3^3\cdot 2 + 3^2\cdot 3 + 3\cdot 4 + 5$

$x_6 = 3x_5 + 6$
$= 3(3^4 + 3^3\cdot 2 + 3^2\cdot 3 + 4\cdot 3 + 5) + 6$
$= 3^5 + 3^4\cdot 2 + 3^3\cdot 3 + 3^2\cdot 4 + 3\cdot 5 + 6$

$\vdots$

Guess:

$x_n = 3^{n-1} + 3^{n-2}\cdot 2 + 3^{n-3}\cdot 3 + \cdots + 3(n-1) + n$
$= 3^{n-1} + \underbrace{3^{n-2} + 3^{n-2}}_{2 \text{ times}} + \underbrace{3^{n-3} + 3^{n-3} + 3^{n-3}}_{3 \text{ times}} +$
$\underbrace{3 + 3 + \cdots + 3}_{(n-1) \text{ times}} + \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$
$= (3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1)$
$+ (3^{n-2} + 3^{n-3} + \cdots + 3^2 + 3 + 1) + \cdots$
$+ (3^2 + 3 + 1) + (3 + 1) + 1$
$= \dfrac{3^n - 1}{2} + \dfrac{3^{n-1} - 1}{2} + \cdots + \dfrac{3^3 - 1}{2}$
$+ \dfrac{3^2 - 1}{2} + \dfrac{3 - 1}{2}$
$= \frac{1}{2}[(3^n + 3^{n-1} + \cdots + 3^2 + 3) - n]$
$= \frac{1}{2}[3(3^{n-1} + 3^{n-2} + \cdots + 3 + 1) - n]$
$= \frac{1}{2}\left(3\left(\dfrac{3^n - 1}{3 - 1}\right) - n\right)$
$= \frac{1}{4}(3^{n+1} - 3 - 2n)$

18. Proof (by mathematical induction): Let d be any fixed constant, and let $a_0, a_1, a_2, \ldots$ be the sequence defined recursively by $a_k = a_{k-1} + d$ for each integer $k \geq 1$. The property $P(n)$ is the equation $a_n = a_0 + nd$. We show by mathematical induction that $P(n)$ is true for every integer $n \geq 0$.

Show that P(0) is true:

When $n = 0$, the left-hand side of the equation is a_0, and the right-hand side is $a_0 + 0\cdot d = a_0$, which equals the left-hand side. Thus $P(0)$ is true.

Show that for every integer k ≥ 0, if P(k) is true, then P(k + 1) is true:

Suppose k is any integer such that $k \geq 0$ and

$$a_k = a_0 + kd.$$

[This is the inductive hypothesis.]

We must show that $a_{k+1} = a_0 + (k+1)d$. Now

$a_{k+1} = a_k + d$ by definition of $a_0, a_1, a_2, \ldots$
$= [a_0 + kd] + d$ by substitution from the inductive hypothesis
$= a_0 + (k+1)d$ by basic algebra

[as was to be shown].

19. Let U_n = the number of units produced on day n. Then

$U_k = U_{k-1} + 2$ for each integer $k \geq 1$,
$U_0 = 170$.

Hence $U_0, U_1, U_2, \ldots$ is an arithmetic sequence with fixed constant 2. It follows that when $n = 30$,

$U_n = U_0 + n\cdot 2 = 170 + 2n = 170 + 2\cdot 30$
$= 230$ units.

Thus the worker must produce 230 units on day 30.

24. $\sum_{k=0}^{20} 5^k = \frac{5^{21} - 1}{4} \cong 1.192 \times 10^{14} \cong$ 119,200,000,000,000 ≅ 119 trillion people (This is about 20,000 times the current population of the earth!)

26. b. *Hint:* Before simplification,
$A_n = 1{,}000(1.0025)^n + 200[(1.0025)^{n-1} + (1.0025)^{n-1} + \cdots + (1.0025)^2 + 1.0025 + 1]$.

d. $A_{240} \cong \$67{,}481.15$, $A_{480} \cong \$188{,}527.05$

e. *Hint:* Use logarithms to solve the equation $A_n = 10{,}000$, where A_n is the expression found after simplifying the result in part (b).

27. a. *Hint:* APY ≅ 19.6%

c. *Hint:* approximately two years

28. Proof (by mathematical induction): Let $a_0, a_1, a_2, \ldots$ be the sequence defined recursively by $a_0 = 1$ and $a_k = ka_{k-1}$ for each integer $k \geq 1$, and let the property $P(n)$ be the equation $a_n = n!$. We show by

mathematical induction that $P(n)$ is true for every integer $n \geq 0$.

Show that P(0) is true:

When $n = 0$, the right-hand side of the equation is $0! = 1$, and by definition of $a_0, a_1, a_2, \ldots$, the left-hand side of the equation, a_0, is also 1. Thus the property is true for $n = 0$.

Show that for every integer k ≥ 0, if P(k) is true, then P(k + 1) is true:

Suppose k is any integer with $k \geq 0$ and

$$a_k = k!.$$

[This is the inductive hypothesis.]

We must show that $a_{k+1} = (k+1)!$. Now

$a_{k+1} = (k+1) \cdot a_k$ by definition of $a_0, a_1, a_2, \ldots$

$= (k+1) \cdot k!$ by substitution from the inductive hypotheses

$= (k+1)!$ by definition of factorial.

[Hence if P(k) is true, then P(k + 1) is true.]

30. Proof (by mathematical induction): Let $c_1, c_2, c_3, \ldots$ be the sequence defined recursively by $c_1 = 1$ and $c_k = 3c_{k-1} + 1$ for each integer $k \geq 2$.

Let the property $P(n)$ be the equation $c_n = \frac{3^n - 1}{2}$. We show by mathematical induction that $P(n)$ is true for every integer $n \geq 1$.

Show that P(1) is true:

When $n = 1$, the right-hand side of the equation is $\frac{3^1 - 1}{2} = \frac{3-1}{2} = 1$, and by definition of $c_1, c_2, c_3, \ldots$, the left-hand side of the equation, c_1, is also 1. Thus the property is true for $n = 1$.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

Suppose that k is any integer with $k \geq 1$ and

$$c_k = \frac{3^k - 1}{2}.$$

[This is the inductive hypothesis.]

We must show that $c_{k+1} = \frac{3^{k+1} - 1}{2}$. Now

$c_{k+1} = 3c_k + 1$ by definition of $c_1, c_2, c_3, \ldots$

$= 3\left(\frac{3^k - 1}{2}\right) + 1$ by substitution from the inductive hypothesis

$= \frac{3^{k+1} - 3}{2} + \frac{2}{2}$

$= \frac{3^{k+1} - 1}{2}$ by basic algebra.

35. *Hint:*

$$2^{k+1} - \frac{2^{k+1} - (-1)^{k+1}}{3}$$

$$= \frac{3 \cdot 2^{k+1}}{3} - \frac{2^{k+1} - (-1)^{k+1}}{3}$$

$$= \frac{2 \cdot 2^{k+1} + (-1)^{k+1}}{3} = \frac{2^{k+2} - (-1)^{k+2}}{3}$$

37. *Hint:*

$$[3 + k(k+1)] + 2(k+1)$$

$$= 3 + k^2 + k + 2k + 2 = 3 + [k^2 + 3k + 2]$$

$$= 3 + (k+1)(k+2)$$

$$= 3 + (k+1)[(k+1) + 1]$$

39. Proof (by mathematical induction): Let $x_1, x_2, x_3, \ldots$ be the sequence defined recursively by $x_1 = 1$ and $x_k = 3x_{k-1} + k$ for each integer $k \geq 2$. Let the property, $P(n)$, be the equation $x_n = \frac{3^{n+1} - 2n - 3}{4}$. We show by mathematical induction that $P(n)$ is true for every integer $n \geq 1$.

Show that P(1) is true:

When $n = 1$, the right-hand side of the equation is $\frac{3^{1+1} - 2 \cdot 1 - 3}{4} = \frac{3^2 - 2 - 3}{4} = 1$, and by definition of $x_1, x_2, x_3, \ldots$, the left-hand side of the equation, x_1, is also 1. Thus $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

Suppose that k is any integer with $k \geq 0$ and $x_k = \frac{3^{k+1} - 2k - 3}{4}$. *[Inductive hypothesis]* We must show that

$x_{k+1} = \frac{3^{(k+1)+1} - 2(k+1) - 3}{}$, or, equivalently,

$x_{k+1} = \frac{3^{k+2} - 2k - 5}{4}$. Now

$x_{k+1} = 3x_k + k$ by definition of $x_1, x_2, x_3,$

$= 3\left(\frac{3^{k+1} - 2k - 3}{4}\right) + k + 1$ by inductive hypothesis

$= \frac{3 \cdot 3^{k+1} - 3 \cdot 2k - 3 \cdot 3}{4} + \frac{4(k+1)}{4}$

$= \frac{3^{k+2} - 6k - 9 + 4k + 4}{4}$

$= \frac{3^{k+2} - 2k - 5}{4}$ by algebra

[as was to be shown].

43 a. $a_0 = 2$

$$a_1 = \frac{a_0}{2a_0 - 1} = \frac{2}{2\cdot 2 - 1} = \frac{2}{3}$$

$$a_2 = \frac{a_1}{2a_1 - 1} = \frac{\frac{2}{3}}{2\cdot\frac{2}{3} - \frac{3}{3}} = \frac{\frac{2}{3}}{\frac{1}{3}} = 2$$

$$a_3 = \frac{a_2}{2a_2 - 1} = \frac{2}{2\cdot 2 - 1} = \frac{2}{3}$$

$$a_4 = \frac{a_3}{2a_3 - 1} = \frac{\frac{2}{3}}{2\cdot\frac{2}{3} - \frac{3}{3}} = \frac{\frac{2}{3}}{\frac{1}{3}} = 2$$

Guess: $a_n = \begin{cases} 2 & \text{if } n \text{ is even} \\ \frac{2}{3} & \text{if } n \text{ is odd} \end{cases}$.

b. Proof (by strong mathematical induction): Let a_0, a_1, a_2, … be the sequence defined recursively by $x_0 = 2$ and $a_k = \frac{a_{k-1}}{2a_{k-1} - 1}$ for each integer $k \geq 1$. Let the property, $P(n)$, be the equation

$$a_n = \begin{cases} 2 & \text{if } n \text{ is even} \\ \frac{2}{3} & \text{if } n \text{ is odd.} \end{cases}$$

We show by strong mathematical induction that $P(n)$ is true for every integer $n \geq 1$.

Show that P(0) and P(1) are true:

The results of part (a) show that $P(0)$ and $P(1)$ are true.

Show that for every integer k ≥ 0, if P(k) is true for each integer i with 0 ≤ i ≤ k, then P(k + 1) is true:

Let k be any integer with $k \geq 0$, and suppose that for each integer i with $0 \leq i \leq k$,

$$a_i = \begin{cases} 2 & \text{if } i \text{ is even} \\ \frac{2}{3} & \text{if } i \text{ is odd.} \end{cases} \quad \textit{[Inductive hypothesis]}$$

We must show that

$$a_{k+1} = \begin{cases} 2 & \text{if } k \text{ is even} \\ \frac{2}{3} & \text{if } k \text{ is odd.} \end{cases}$$

Now

$$a_{k+1} = \frac{a_k}{2a_k - 1} \qquad \text{by definition of } a_0, a_1, a_2, \ldots$$

$$= \begin{cases} \frac{2}{2\cdot 2 - 1} & \text{if } k \text{ is even} \\ \frac{\frac{2}{3}}{2\cdot\frac{2}{3} - 1} & \text{if } k \text{ is odd} \end{cases} \qquad \text{by inductive hypothesis}$$

$$= \begin{cases} \frac{2}{3} & \text{if } k \text{ is even} \\ \frac{\frac{2}{3}}{\frac{1}{3}} & \text{if } k \text{ is odd} \end{cases}$$

$$= \begin{cases} \frac{2}{3} & \text{if } k+1 \text{ is odd} \\ 2 & \text{if } k+1 \text{ is even} \end{cases} \qquad \begin{array}{l} \text{because } k+1 \text{ is odd when } k \text{ is even} \\ \text{and } k+1 \text{ is even when } k \text{ is odd} \end{array}$$

[as was to be shown].

45. $v_1 = 1$

$$\begin{aligned} v_2 &= v_{\lfloor 2/2 \rfloor} + v_{\lfloor 3/2 \rfloor} + 2 = v_1 + v_1 + 2 \\ &= 1 + 1 + 2 \\ v_3 &= v_{\lfloor 3/2 \rfloor} + v_{\lfloor 4/2 \rfloor} + 2 = v_1 + v_2 + 2 \\ &= 1 + (1 + 1 + 2) + 2 = 3 + 2\cdot 2 \\ v_4 &= v_{\lfloor 4/2 \rfloor} + v_{\lfloor 5/2 \rfloor} + 2 = v_2 + v_2 + 2 \\ &= (1 + 1 + 2) + (1 + 1 + 2) + 2 \\ &= 4 + 3\cdot 2 \\ v_5 &= v_{\lfloor 5/2 \rfloor} + v_{\lfloor 6/2 \rfloor} + 2 = v_2 + v_3 + 2 \\ &= (3 + 2\cdot 2) + (1 + 1 + 2) + 2 \\ &= 5 + 4\cdot 2 \\ v_6 &= v_{\lfloor 6/2 \rfloor} + v_{\lfloor 7/2 \rfloor} + 2 = v_3 + v_3 + 2 \\ &= (3 + 2\cdot 2) + (3 + 2\cdot 2) + 2 \\ &= 6 + 5\cdot 2 \\ &\vdots \end{aligned}$$

Guess:

$v_n = n + 2(n - 1) = 3n - 2$ for every integer $n \geq 1$

b. Proof (by strong mathematical induction): Let v_1, v_2, v_3, … be the sequence defined recursively by $v_1 = 1$ and $v_k = v_{\lfloor k/2 \rfloor} + v_{\lfloor (k+1)/2 \rfloor} + 2$ for each integer $k \geq 1$. Let the property, $P(n)$, be the equation

$$v_n = 3n - 2.$$

We show by strong mathematical induction that $P(n)$ is true for every integer $n \geq 1$.

Show that P(1) is true:

When $n = 1$, the right-hand side of the equation is $3\cdot 1 - 2 = 1$, which equals v_1 by definition of v_1, v_2, v_3, …. Thus $P(1)$ is true.

Show that for every integer k ≥ 1, if P(i) is true for each integer i with 0 ≤ i ≤ k, then P(k + 1) is true:

Let k be any integer with $k \geq 1$, and suppose that for each integer i with $1 \leq i \leq k$, $v_i = 3i - 2$.

[This is the inductive hypothesis.] We must show that $v_{k+1} = 3(k+1) - 2 = 3k + 1$.

$$
\begin{aligned}
v_{k+1} &= v_{\lfloor (k+1)/2 \rfloor} + v_{\lfloor (k+2)/2 \rfloor} + 2 && \text{by definition of } v_1, v_2, v_3, \ldots \\
&= \left(3\left\lfloor \frac{k+1}{2} \right\rfloor - 2\right) + \left(3\left\lfloor \frac{k+2}{2} \right\rfloor - 2\right) + 2 \\
&= 3\left(\left\lfloor \frac{k+1}{2} \right\rfloor + \left\lfloor \frac{k+2}{2} \right\rfloor\right) - 2 \\
&= \begin{cases} 3\left(\dfrac{k}{2} + \dfrac{k+2}{2}\right) - 2 & \text{if } k \text{ is even} \\ 3\left(\dfrac{k+1}{2} + \dfrac{k+1}{2}\right) - 2 & \text{if } k \text{ is odd} \end{cases} \\
&= 3\left(\frac{2k+2}{2}\right) - 2 \\
&= 3(k+1) - 2 \\
&= 3k + 1 && \text{by the laws of algebra}
\end{aligned}
$$

[as was to be shown].

46. *Hint:* Show that for every integer $n \geq 0$, $s_{2n} = 2^n$ and $s_{2n+1} = 2^{n+1}$. Then combine these formulas using the ceiling function to obtain $s_n = 2^{\lceil n/2 \rceil}$.

48. a. *Hint:*

$$w_n = \begin{cases} \left(\dfrac{n+1}{2}\right)^2 & \text{if } n \text{ is odd} \\ \dfrac{n}{2}\left(\dfrac{n}{2} + 1\right) & \text{if } n \text{ is even} \end{cases}$$

49. a. *Hint:* Express the answer using the Fibonacci sequence.

50. Performing the inductive step for a proof by mathematical induction of the formula, involves substituting $(k-2)^2$ in place of a_{k-1} in the expression $a_k = 2a_{k-1} + k - 1$ in hopes of showing that a_k equals $(k-1)^2$. However, solving $2(k-2)^2 + k - 1 = (k-1)^2$ for k, gives that $k - 5k + 6 = 0$, which implies that $k = 2$ or $k = 3$. It turns out that the sequence a_1, a_2, a_3 ,… does satisfy the given formula for $k = 2$ and $k = 3$, but when $k = 4$, $a_4 = 2 \cdot 4 + (4 - 1) = 11$, and $11 \neq (4-1)^2$. Hence the sequence does not satisfy the formula for $n = 4$.

52. a. *Hint:* The maximum number of regions is obtained when each additional line crosses all the previous lines, but not at any point that is already the intersection of two lines. When a new line is added, it divides each region through which it passes into two pieces. The number of regions a newly added line passes through is one more than the number of lines it crosses.

53. *Hint:* The answer involves the Fibonacci numbers!

SECTION 5.8

1. (a), (d), and (f)

3. a. $\left.\begin{aligned} a_0 &= C \cdot 2^0 + D = C + D = 1 \\ a_1 &= C \cdot 2^1 + D = 2C + D = 3 \end{aligned}\right\}$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 2C + (1 - C) &= 3 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} C &= 2 \\ D &= -1 \end{aligned}\right.$$

$a_2 = 2 \cdot 2^2 + (-1) = 7$

4. a. $\left.\begin{aligned} b_0 &= C \cdot 3^0 + D \cdot (-2)^0 = C + D = 0 \\ b_1 &= C \cdot 3^1 + D \cdot (-2)^1 = 3C - 2D = 5 \end{aligned}\right\}$

$$\Leftrightarrow \left\{\begin{aligned} D &= -C \\ 3C - 2(-C) &= 5 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} C &= 1 \\ D &= -1 \end{aligned}\right.$$

$b_2 = 3^2 + (-1)(-2)^2 = 9 - 4 = 5$

5. Proof: Given that $a_n = C \cdot 2^n + D$, then for any choice of C and D and an integer $k > 2$,

$$
\begin{aligned}
a_k &= C \cdot 2^k + D \\
a_{k-1} &= C \cdot 2^{k-1} + D \\
a_{k-2} &= C \cdot 2^{k-2} + D.
\end{aligned}
$$

Hence

$$
\begin{aligned}
3a_{k-1} - 2a_{k-2} &= 3(C \cdot 2^{k-1} + D) - 2(C \cdot 2^{k-2} + D) \\
&= 3C \cdot 2^{k-1} + 3D - 2C \cdot 2^{k-2} - 2D \\
&= 3C \cdot 2^{k-1} - C \cdot 2^{k-1} + D \\
&= 2C \cdot 2^{k-1} + D \\
&= C \cdot 2^k + D = a_k.
\end{aligned}
$$

8. a. If, for each $k > 2$, $t^k = 2t^{k-1} + 3t^{k-2}$ and $t \neq 0$, then $t^2 = 2t + 3$ *[by dividing by t^{k-2}]*, and so $t^2 - 2t - 3 = 0$. And, since $t^2 - 2t - 3 = (t-3)(t+1)$, then $t = 3$ or $t = -1$.

b. It follows from (a) and the distinct roots theorem that for some constants C and D, a_0, a_1, a_2, … satisfies the equation

$a_n = C \cdot 3^n + D \cdot (-1)^n$ for every integer $n \geq 0$.

Since $a_0 = 1$ and $a_1 = 2$, then

$$\left.\begin{aligned} a_0 &= C \cdot 3^0 + D \cdot (-1)^0 = C + D = 1 \\ a_1 &= C \cdot 3^1 + D \cdot (-1)^1 = 3C - D = 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 3C - (1 - C) &= 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 4C - 1 &= 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} C &= 3/4 \\ D &= 1/4. \end{aligned}\right.$$

Thus $a_n = \frac{3}{4}(3^n) + \frac{1}{4}(-1)^n$ for every integer $n \geq 0$.

11. *Characteristic equation:* $t^2 - 4 = 0$. Since $t^2 - 4 = (t-2)(t+2)$, $t = 2$ and $t = -2$ are the roots. By the distinct roots theorem, for some constants C and D

$$d_n = C\cdot(2^n) + D\cdot(-2)^n \quad \text{for every integer } n \geq 0.$$

Since $d_0 = 1$ and $d_1 = -1$, then

$$\left.\begin{aligned} d_0 &= C\cdot 2^0 + D\cdot(-2)^0 = C + D = 1 \\ d_1 &= C\cdot 2^1 + D\cdot(-2)^1 = 2C - 2D = -1 \end{aligned}\right\}$$

$$\Leftrightarrow \begin{cases} D = 1 - C \\ 2C - 2(1-C) = -1 \end{cases}$$

$$\Leftrightarrow \begin{cases} D = 1 - C \\ 4C - 2 = -1 \end{cases}$$

$$\Leftrightarrow \begin{cases} C = \frac{1}{4} \\ D = \frac{3}{4}. \end{cases}$$

Thus $d_n = \frac{1}{4}(2^n) + \frac{3}{4}(-2)^n$ for every integer $n \geq 0$.

13. *Characteristic equation:* $t^2 - 2t + 1 = 0$. By the quadratic formula,

$$t = \frac{2 \pm \sqrt{4 - 4\cdot 1}}{2} = \frac{2}{2} = 1.$$

By the single root theorem, for some constants C and D

$$\begin{aligned} r_n &= C\cdot(1^n) + Dn\cdot(1^n) \\ &= C + nD \quad \text{for every integer } n \geq 0. \end{aligned}$$

Since $r_0 = 1$ and $r_1 = 4$, then

$$\left.\begin{aligned} r_0 &= C + 0\cdot D = C = 1 \\ r_1 &= C + 1\cdot D = C + D = 4 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} C &= 1 \\ 1 + D &= 4 \end{aligned}\right\}$$

$$\Leftrightarrow \begin{cases} C = 1 \\ D = 3. \end{cases}$$

Thus $r_n = 1 + 3n$ for every integer $n \geq 0$.

16. *Hint:* For every integer $n \geq 0$,

$$s_n = \frac{\sqrt{3}+2}{2\sqrt{3}}(1+\sqrt{3})^n + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^n.$$

19. Proof: Suppose r, s, a_0, and a_1 are numbers with $r \neq s$. Consider the system of equations

$$\begin{aligned} C + D &= a_0 \\ Cr + Ds &= a_1. \end{aligned}$$

By solving for D and substituting, we find that

$$\begin{aligned} D &= a_0 - C \\ Cr + (a_0 - C)s &= a_1. \end{aligned}$$

Hence

$$C(r-s) = a_1 - a_0 s.$$

Since $r \neq s$, both sides may be divided by $r - s$. Thus the given system of equations has the unique solution

$$C = \frac{a_1 - a_0 s}{r - s}$$

and

$$\begin{aligned} D = a_0 - C &= a_0 - \frac{a_1 - a_0 s}{r - s} \\ &= \frac{a_0 r - a_0 s - a_1 + a_0 s}{r - s} = \frac{a_0 r - a_1}{r - s}. \end{aligned}$$

Alternative solution: Since the determinant of the system is $1\cdot s - r\cdot 1 = s - r$ and since $r \neq s$, the given system has nonzero determinant and therefore has a unique solution.

21. *Hint:* Use strong mathematical induction. First note that the formula holds for $n = 0$ and $n = 1$. To prove the inductive step, suppose that k is any integer such that $k \geq 2$ and the formula holds for every integer i with $0 \leq i \leq k$. Then show that the formula holds for $k + 1$. Use the proof of Theorem 5.8.3 (the distinct roots theorem) as a model.

22. The characteristic equation is $t^2 - 2t + 2 = 0$. By the quadratic formula, its roots are

$$t = \frac{2 \pm \sqrt{4-8}}{2} = \frac{2 \pm 2i}{2} = \begin{cases} 1+i \\ 1-i. \end{cases}$$

By the distinct roots theorem, for some constants C and D

$$a_n = C(1+i)^n + D(1-i)^n$$

for every integer $n \geq 0$.

Since $a_0 = 1$ and $a_1 = 2$, then

$$a_0 = C(1+i)^0 + D(1-i)^0 = C + D = 1$$

$$\begin{aligned} a_1 &= C(1+i)^1 + D(1-i)^1 \\ &= C(1+i) + D(1-i) = 2 \end{aligned}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C(1+i) + (1-C)(1-i) &= 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C(1+i-1+i) + 1 - i &= 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C(2i) &= 1 + i \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C &= \frac{1+i}{2i} = \frac{1+i}{2i}\cdot\frac{i}{i} = \frac{i-1}{-2} = \frac{1-i}{2} \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - \frac{1-i}{2} = \frac{2-1+i}{2} = \frac{1+i}{2} \\ C &= \frac{1-i}{2} \end{aligned}\right\}.$$

Thus for every integer, $n \geq 0$,

$$a_n = \left(\frac{1-i}{2}\right)(1+i)^n + \left(\frac{1+i}{2}\right)(1-i)^n.$$

SECTION 5.9

1. a. (1) p, q, r, and s are Boolean expressions by I.
(2) $\sim s$ is a Boolean expression by (1) and II(c).
(3) $r \vee \sim s$ is a Boolean expression by (1), (2), and II(b).
(4) $(r \vee \sim s)$ is a Boolean expression by (3) and II(d).
(5) $q \wedge (r \vee \sim s)$ is a Boolean expression by (1), (4), and II(a)
(6) $(q \wedge (r \vee \sim s))$ is a Boolean expression by (5) and II(d)
(7) $\sim p$ is a Boolean expression by (1) and II(c).
(8) $\sim p \vee (q \wedge (r \vee \sim s))$ is a Boolean expression by (6), (7), and II(b).

2. a. (1) ( ) is in C by I.
(2) (( )) is in C by (1) and II(a).
(3) ( )(( )) is in C by (1), (2), and II(b).

3. a. (1) By Theorem 5.9.1, a and b are strings in S because a and b are in A.
(2) By (1) and part II(c) of the definition of string, $a(bc) = (ab)c$ because a and b are strings in S and c is in A.

4. a. (1) MI is in the MIU system by I.
(2) MII is in the MIU system by (1) and II(b).
(3) $MIIII$ is in the MIU system by (3) and II(b).
(4) $MIIIIIIII$ is in the MIU system by (3) and II(b).
(5) $MIUIIII$ is in the MIU system by (4) and II(c).
(6) $MIUUI$ is in the MIU system by (5) and II(c).
(7) $MIUI$ is in the MIU system by (6) and II(d).

5. a. (1) 2, 0.3, 4.2, and 7 are arithmetic expressions by I.
(2) $(0.3 - 4.2)$ is an arithmetic expression by (1) and II(d).
(3) $(2 \cdot (0.3 - 4.2))$ is an arithmetic expression by (1), (2), and II(e).
(4) (-7) is an arithmetic expression by (1) and II(b).
(5) $((2 \cdot (0.3 - 4.2)) + (-7))$ is an arithmetic expression by (3), (4), and II(c).

6. Proof (by structural induction): By the definition of S in exercise 6, the only integer in the base for S is 5, and the recursion rule states that for every integer n in S, $n + 4$ is in S. Given any integer n in S, let property $P(n)$ be the sentence, "$n \bmod 2 = 1$."

Show that P(n) is true for each integer n in the base for S:

The only integer in the base for S is 5, and $P(5)$ is true because $5 \bmod 2 = 1$ since $5 = 2 \cdot 2 + 1$.

Show that for each integer n in S, if P(n) is true and if m is obtained from n by applying a rule from the recursion for S, then P(m) is true:

Suppose n is any integer in S such that $P(n)$ is true, or, in other words, $n \bmod 2 = 1$. *[This is the inductive hypothesis.]* The recursion for S consists of only one rule, and when the rule is applied to n, the result is $n + 4$. To complete the inductive step, we must show that $P(n + 4)$ is true, or, equivalently, that $(n + 4) \bmod 2 = 1$. Now since $n \bmod 2 = 1$, then

$$n = 2k + 1 \text{ for some integer } k.$$

Hence

$$\begin{aligned} (n+4) \bmod 2 &= [(2k+1)+4] \bmod 2 && \text{by substitution} \\ &= [2(k+2)+1] \bmod 2 && \text{by basic algebra} \\ &= 1 && \text{because } k+2 \text{ is an integer,} \end{aligned}$$

and so $P(n + 4)$ is true *[as was to be shown]*.

Conclusion: Because there are no integers in S other than those obtained from the base and the recursion for S, we conclude that every integer n in S satisfies the equation $n \bmod 2 = 1$.

7. Proof (by structural induction): By the definition of S in exercise 7, the only element in the base is 1, and the recursion rules II(a) and II(b) state that for every string s in S, $0s$ and $1s$ are in S. Given any string s in S, let property $P(s)$ be the sentence "s ends in a 1."

Show that P(a) is true for each string a in the base for S:

The only string in the base for S is 1, which ends in a 1, and so $P(1)$ is true.

Show that for each string x in S, if P(x) is true and if y is obtained from x by applying a rule from the recursion for S, then P(y) is true:

The recursion for S consists of two rules: II(a) and II(b). Suppose s is any string in S such that $P(s)$ is true, which means that s ends in a 1. *[This is the inductive hypothesis.]* To complete the inductive step, we must show that applying either of the two recursion rules to s also results in a string that ends in 1.

Now when rule II(a) is applied to s, the result is $0s$ and when rule II(b) is applied to s, the result is $1s$. Because s ends in a 1, so do $0s$ and $1s$, which means that $P(0s)$ and $P(1s)$ are true and completes the inductive step.

Conclusion: Because there are no strings in S other than those obtained from the base and recursion for S, we conclude that every string in S ends in a 1.

9. Proof (by structural induction): By the definition of S in exercise 9, the only element in the base is λ, and the recursion rules II(a)–II(d) state that for every string s in S, bs, sb, saa, and aas are in S. Given any string, s in S, let property $P(s)$ be the sentence "s contains an even number of a's."

Show that P(a) is true for each string a in the base for S:

The only string in the base for S is λ, which contains 0 a's. Since 0 is an even number, $P(\lambda)$ is true.

Show that for each string x in S, if P(x) is true and if y is obtained from x by applying a rule from the recursion for S, then P(y) is true:

Suppose s is a string in S such that $P(s)$ is true, or, in other words, suppose that s has an even number of a's. *[This is the inductive hypothesis.]*

When either rule II(a) or II(b) is applied to s, the result is either bs or sb, each of which contains the same number of a's as s and hence an even number of a's. Thus both $P(bs)$ and $P(sb)$ are true.

When either rule II(c) or II(d) is applied to s, the result is either aas or saa, each of which contains two more a's than does s. Because two more than an even number is an even number, both aas and saa contain an even number of a's. Hence both $P(aas)$ and $P(saa)$ are true. This completes the inductive step because II(a)–II(d) are the only rules in the recursion.

Conclusion: Because there are no strings in S other than those obtained from the base and the recursion for S, we conclude that every string in S contains an even number of a's.

10. *Hint:* For each string s in S, let property $P(s)$ be the sentence: "s represents an odd integer." In the decimal notation, a string represents an odd integer if, and only if, it ends in 1, 3, 5, 7, or 9.

11. *Hint:* By divisibility results from Chapter 4 (exercises 15 and 16 of Section 4.4), if both k and m are divisible by 5, then so are $k+m$ and $k-m$.

13. *Hint:* Can the number of I's in a string in the $M\,I\,U$ system be a multiple of 3? How do rules II(a)–II(d) affect the number of I's in a string?

15. a. The parenthesis structure ( )(( ) is not in C. To see why this is so, we will prove that every parenthesis structure in C has an equal number of left and right parentheses. It will follow that, since ( )(( ) has 3 left parentheses and 2 right parentheses, ( )(( ) cannot be in C.

Proof (by structural induction):

Define a function $f : C \to \mathbf{Z}$ as follows: For each parenthesis structure x in C, let

$$f(x) = \begin{bmatrix}\text{the number of left}\\ \text{parentheses in } x\end{bmatrix} - \begin{bmatrix}\text{the number of right}\\ \text{parentheses in } x\end{bmatrix}.$$

Given any parenthesis structure x in C, let property $P(x)$ be the sentence, "$f(x) = 0$."

Show that P(a) is true for each parenthesis structure a in the base for C:

The only parenthesis structure in the base for C is ( ), and $f[(\,)] = 0$ because ( ) has one left parenthesis and one right parenthesis. Hence $P[(\,)]$ is true.

Show that for each parenthesis structure x in C, if P(x) is true and if y is obtained from x by applying a rule from the recursion for C, then P(y) is true:

The recursion for C consists of two rules, denoted II(a) and II(b).

Suppose u and v are any parenthesis structures in C such that $P(u)$ and $P(v)$ are true. This means that $f(u) = 0$ and $f(v) = 0$. *[This is the inductive hypothesis.]*

Let k and m be the numbers of left and right parentheses, respectively, in u, and let n and p be the numbers of left and right parentheses, respectively, in v. Then $k - m = 0$ and $n - p = 0$ by definition of f.

When rule II(a) is applied to u, the result is (u), and $f[(u)] = 0$ because (u) has one more left parenthesis and one more right parenthesis than u, and $(k+1) - (m+1) = 0$. Hence, $P(u)$ is true.

When rule II(b) is applied to u and v, the result is uv. Now uv has $k+n$ left parentheses and $m+p$ right parentheses. Hence $f(uv) = (k+n) - (m+p) = (k-m) + (n-p) = 0 + 0 = 0$. Hence, $f(uv) = 0$, and so $P(uv)$ is true.

Conclusion: Because there are no parenthesis structures in C other than those obtained from the base and the recursion for C, we conclude that given any parenthesis structure x in C, $f(x) = 0$. Therefore, every parenthesis structure in C has the same number of left and right parentheses.

b. *Hint:* This parenthesis structure is not in C either even though it has equal numbers of left and right parentheses.

16. Let S be the set of all strings of 0's and 1's with the same number of 0's and 1's. The following is a recursive definition for S.

I. Base: The null string $\lambda \in S$.

II. Recursion: If $s \in S$, then

a. $01s \in S$ **b.** $s01 \in S$ **c.** $10s \in S$
d. $s10 \in S$ **e.** $0s1 \in S$ **f.** $1s0 \in S$

III. Restriction: There are no elements of S other that those obtained from the base and recursion for S.

18. Let T be the set of all strings of a's and b's that contain an odd number of a's. The following is a recursive definition of T.

I. Base: $a \in T$.

II. Recursion: If $t \in T$, then

a. $bt \in T$ **b.** $tb \in T$ **c.** $aat \in T$

d. $ata \in T$ **e.** $taa \in T$

III. Restriction: There are no elements of T other than those obtained from the base and recursion for T.

20. a. Suppose a is any character in A. *[We must show that $L(a) = 1$.]* Then

$$\begin{aligned} L(a) &= L(\lambda \cdot a) && \text{by part II(b) of the definition of string} \\ &= L(\lambda) + 1 && \text{by part (b) of the definition of the length function} \\ &= 0 + 1 && \text{by part (a) of the definition of the length function} \\ &= 1 && \text{by definition of 0.} \end{aligned}$$

22. *Hint:* If S is the set of all strings over a finite set A, then for any string u in S, let the property $P(v)$ be the sentence "If v is any string of length n, then $\text{Rev}(uv) = \text{Rev}(v)\text{Rev}(u)$." For the basis step you will show that $P(\lambda)$ is true by showing that $\text{Rev}(u\lambda) = \text{Rev}(\lambda)\text{Rev}(u)$. For the inductive step you will assume that x is any string for which $P(x)$ is true, and you will show that if y is the result of applying rule II(a) to x, then $P(y)$ is true.

23. a.
$$\begin{aligned} M(86) &= M(M(97)) && \text{since } 86 \le 100 \\ &= M(M(M(108))) && \text{since } 97 \le 100 \\ &= M(M(98)) && \text{since } 108 > 100 \\ &= M(M(M(109))) && \text{since } 98 < 100 \\ &= M(M(99)) && \text{since } 109 > 100 \\ &= M(91) && \text{by Example 5.9.7} \end{aligned}$$

25. a.
$$\begin{aligned} A(1, 1) &= A(0, A(1, 0)) && \text{by (5.9.3) with } m = 1 \text{ and } n = 1 \\ &= A(1, 0) + 1 && \text{by (5.9.1) with } n = A(1, 0) \\ &= A(0, 1) + 1 && \text{by (5.9.2) with } m = 1 \\ &= (1 + 1) + 1 && \text{by (5.9.1) with } n = 1 \\ &= 3 \end{aligned}$$

Alternative solution:

$$\begin{aligned} A(1, 1) &= A(0, A(1, 0)) && \text{by (5.9.3) with } m = 1 \text{ and } n = 1 \\ &= A(0, A(0, 1)) && \text{by (5.9.2) with } m = 1 \\ &= A(0, 2) && \text{by (5.9.1) with } n = 1 \\ &= 3 && \text{by (5.9.1) with } n = 2 \end{aligned}$$

26. a. Proof by mathematical induction: Let the property, $P(n)$, be the equation $A(1, n) = n + 2$.

Show that P(0) is true:

When $n = 0$,

$$\begin{aligned} A(1, n) &= A(1, 0) && \text{by substitution} \\ &= A(0, 1) && \text{by (5.9.2)} \\ &= 1 + 1 && \text{by (5.9.1)} \\ &= 2. \end{aligned}$$

On the other hand, $n + 2 = 0 + 2$ also. Thus $A(1, n) = n + 2$ for $n = 0$.

Show that for every integer $k \ge 0$, if $P(k)$ is true, then $P(k + 1)$ is true:

Let k be an integer with $k \ge 1$ and suppose $P(k)$ is true. In other words, suppose $A(1, k) = k + 2$. *[This is the inductive hypothesis.]* We must show that $P(k + 1)$ is true. In other words, we must show that $A(1, k + 1) = (k + 1) + 2 = k + 3$. Now

$$\begin{aligned} A(1, k + 1) &= A(0, A(1, k)) && \text{by (5.9.3)} \\ &= A(1, k) + 1 && \text{by (5.9.1)} \\ &= (k + 2) + 1 && \text{by inductive hypothesis} \\ &= k + 3 \end{aligned}$$

[as was to be shown].

[Since both the basis and the inductive steps have been proved, we conclude that the equation holds for every nonnegative integer n.]

28. Suppose F is a function. Then $F(1) = 1$, $F(2) = F(1) = 1$, $F(3) = 1 + F(5 \cdot 3 - 9) = 1 + F(6) = 1 + F(3)$. Subtracting $F(3)$ from the extreme left and extreme right of this sequence of equations gives $1 = 0$, which is false. Hence F is not a function.

SECTION 6.1

1. a. $A = \{2, \{2\}, (\sqrt{2})^2\} = \{2, \{2\}, 2\} = \{2, \{2\}\}$ and $B = \{2, \{2\}, \{\{2\}\}\}$. So $A \subseteq B$ because every element in A is in B, but $B \not\subseteq A$ because $\{\{2\}\} \in B$ and $\{\{2\}\} \notin A$. Thus A is a proper subset of B.

c. $A = \{\{1, 2\}, \{2, 3\}\}$ and $B = \{1, 2, 3\}$. So $A \not\subseteq B$ because $\{1, 2\} \in A$ and $\{1, 2\} \notin B$. Also $B \not\subseteq A$ because $1 \in B$ and $1 \notin A$.

e. $A = \{\sqrt{16}, \{4\}\} = \{4, \{4\}\}$ and $B = \{4\}$. Then $B \subseteq A$ because the only element in B is 4 and 4 is in A, but $A \not\subseteq B$ because $\{4\} \in A$ and $\{4\} \notin B$. Thus B is a proper subset of A.

2. ***Proof That $B \subseteq A$:***

Suppose x is a particular but arbitrarily chosen element of B.

[We must show that $x \in A$. By definition of A, this means we must show that $x = 2 \cdot$(some integer).]

By definition of B, there is an integer b such that $x = 2b - 2$.

[Given that $x = 2b - 2$, can x also be expressed as $2\cdot$ (some integer)? That is, is there an integer—say, a—such that $2b - 2 = 2a$? Solve for a to obtain $a = b - 1$. Check to see if this works.]

Let $a = b - 1$.

[First check that a is an integer.]

We know that a is an integer because it is a difference of integers.

[Then check that $x = 2a$.]

By substitution, $2a = 2(b - 1) = 2b - 2 = x$.

Thus, by definition of A, x is an element of A,

[as was to be shown].

3. a. $R \not\subseteq T$ because there are elements in R that are not in T. For example, the number 2 is in R but 2 is not in T since 2 is not divisible by 6.

b. $T \subseteq R$ because every element in T is in R since every integer divisible by 6 is divisible by 2. To see why this is so, suppose n is any integer that is divisible by 6. Then $n = 6m$ for some integer m. Since $6m = 2(3m)$ and since $3m$ is an integer (being a product of integers), it follows that $n = 2\cdot$(*some integer*), and, hence, that n is divisible by 2.

5. a. $C \subseteq D$ because every element in C is in D. To see why this is so, suppose n is any element of C. Then $n = 6r - 5$ for some integer r. Let $s = 2r - 2$. Then s is an integer (because products and differences of integers are integers), and

$$3s + 1 = 3(2r - 2) + 1 = 6r - 6 + 1 = 6r - 5,$$

which equals n. Thus n satisfies the condition for being in D. Hence, every element in C is in D.

b. $D \not\subseteq C$ because there are elements of D that are not in C. For example, 4 is in D because $4 = 3\cdot 1 + 1$. But 4 is not in C because if it were, then $4 = 6r - 5$ for some integer r, which would imply that $9 = 6r$, or, equivalently, that $r = 3/2$, and this contradicts the fact that r is an integer.

6. c. ***Sketch of proof that $B \subseteq C$:*** If r is any element of B then there is an integer b such that $r = 10b - 3$. To show that r is in C, you must show that there is an integer c such that $r = 10c + 7$. In scratch work, assume that c exists and use the information that $10b - 3$ would have to equal $10c + 7$ to deduce the only possible value for c. Then show that this value is (1) an integer and (2) satisfies the equation $r = 10c + 7$, which will allow you to conclude that r is an element of C.

Sketch of proof that $C \subseteq B$: If s is any element of C then there is an integer c such that $s = 10c + 7$. To show that s is in B, you must show that there is an integer b such that $s = 10c - 3$. In scratch work, assume that b exists and use the information that $10c + 7$ would have to equal $10b - 3$ to deduce the only possible value for b. Then show that this value is (1) an integer and (2) satisfies the equation $s = 10b - 3$, which will allow you to conclude that s is an element of B.

8. a. *In words:* The set of all x in U such that x is in A and x is in B.

In symbolic notation: $A \cap B$.

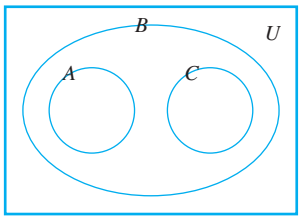
9. a. $x \notin A$ and $x \notin B$

10. a. $A \cup B = \{1, 3, 5, 6, 7, 9\}$
b. $A \cap B = \{3, 9\}$
c. $A \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
d. $A \cap C = \varnothing$
e. $A - B = \{1, 5, 7\}$

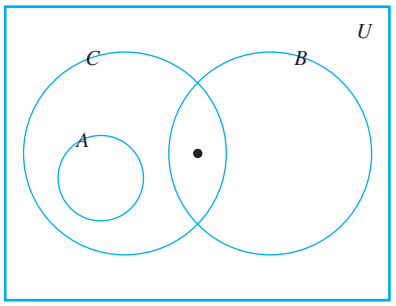
11. a. $A \cup B = \{x \in \mathbf{R} \mid 0 < x < 4\}$
b. $A \cap B = \{x \in \mathbf{R} \mid 1 \le x \le 2\}$
c. $A^c = \{x \in \mathbf{R} \mid x \le 0 \text{ or } x > 2\}$
d. $A \cup C = \{x \in \mathbf{R} \mid 0 < x \le 2 \text{ or } 3 \le x < 9\}$
e. $A \cap C = \varnothing$
f. $B^c = \{x \in \mathbf{R} \mid x < 1 \text{ or } x \ge 4\}$
g. $A^c \cap B^c = \{x \in \mathbf{R} \mid x \le 0 \text{ or } x \ge 4\}$
h. $A^c \cup B^c = \{x \in \mathbf{R} \mid x < 1 \text{ or } x > 2\}$
i. $(A \cap B)^c = \{x \in \mathbf{R} \mid x < 1 \text{ or } x > 2\}$
j. $(A \cup B)^c = \{x \in \mathbf{R} \mid x \le 0 \text{ or } x \ge 4\}$

13. a. $A \cap B = \{1111\}$
c. $A - B = \{1110, 1000, 1001\}$

14. a.



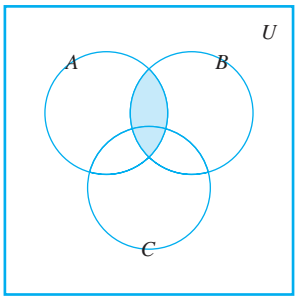
15. a.



16. a. $A \cup (B \cap C) = \{a, b, c\}$, $(A \cup B) \cap C = \{b, c\}$, and $(A \cup B) \cap (A \cup C) = \{a, b, c, d\} \cap \{a, b, c, e\} = \{a, b, c\}$.

Hence $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

17. a.



18. a. The number 0 is not in $\varnothing$ because $\varnothing$ has no elements.

b. No. The left-hand set is the empty set; it does not have any elements. The right-hand set is a set with one element, namely $\varnothing$.

19. $A_1 = \{1, 1^2\} = \{1\}$, $A_2 = \{2, 2^2\} = \{2, 4\}$, $A_3 = \{3, 3^2\} = \{3, 9\}$, $A_4 = \{4, 4^2\} = \{4, 16\}$

a. $A_1 \cup A_2 \cup A_3 \cup A_4 = \{1\} \cup \{2, 4\} \cup \{3, 9\} \cup \{4, 16\} = \{1, 2, 3, 4, 9, 16\}$

b. $A_1 \cap A_2 \cap A_3 \cap A_4 = \{1\} \cap \{2, 4\} \cap \{3, 9\} \cap \{4, 16\} = \varnothing$

c. A_1, A_2, A_3, and A_4 are not mutually disjoint, because $A_2 \cap A_4 = \{4\} = \varnothing$.

21. $C_0 = \{0, -0\} = \{0\}$, $C_1 = \{1, -1\}$, $C_2 = \{2, -2\}$, $C_3 = \{3, -3\}$, $C_4 = \{4, -4\}$

a. $\displaystyle\bigcup_{i=0}^{4} C_i = \{0\} \cup \{1, -1\} \cup \{2, -2\} \cup \{3, -3\} \cup \{4, -4\} = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

b. $\displaystyle\bigcap_{i=0}^{4} C_i = \{0\} \cap \{1,-1\} \cap \{2,-2\} \cap \{3,-3\} \cap \{4, -4\} = \varnothing$

c. $C_0, C_1, C_2, \ldots$ are mutually disjoint because no two of the sets have any elements in common.

d. $\displaystyle\bigcup_{i=0}^{n} C_i = \{-n, -(n-1), \ldots, -2, -1, 0, 1, 2, \ldots, (n-1), n\}$

e. $\displaystyle\bigcap_{i=0}^{n} C_i = \varnothing$

f. $\displaystyle\bigcup_{i=0}^{\infty} C_i = \mathbf{Z}$, the set of all integers

g. $\displaystyle\bigcap_{i=0}^{\infty} C_i = \varnothing$

22. $D_0 = [-0, 0] = \{0\}$, $D_1 = [-1, 1]$, $D_2 = [-2, 2]$, $D_3 = [-3, 3]$, $D_4 = [-4, 4]$

a. $\displaystyle\bigcup_{i=0}^{4} D_i = \{0\} \cup [-1, 1] \cup [-2, 2] \cup [-3, 3] \cup [-4, 4] = [-4, 4]$

b. $\displaystyle\bigcap_{i=0}^{4} D_i = \{0\} \cap [-1, 1] \cap [-2, 2] \cap [-3, 3] \cap [-4, 4] = \{0\}$

c. $D_0, D_1, D_2, \ldots$, are not mutually disjoint. In fact, each $D_k \subseteq D_{k+1}$.

d. $\displaystyle\bigcup_{i=0}^{n} D_i = [-n, n]$

e. $\displaystyle\bigcap_{i=0}^{n} D_i = \{0\}$

f. $\displaystyle\bigcup_{i=0}^{\infty} D_i = \mathbf{R}$, the set of all real numbers

g. $\displaystyle\bigcap_{i=0}^{\infty} D_i = \{0\}$

24. $W_0 = (0, \infty)$, $W_1 = (1, \infty)$, $W_2 = (2, \infty)$, $W_3 = (3, \infty)$, $W_4 = (4, \infty)$

a. $\displaystyle\bigcup_{i=0}^{4} W_i = (0, \infty) \cup (1, \infty) \cup (2, \infty) \cup (3, \infty) \cup (4, \infty) = (0, \infty)$

b. $\displaystyle\bigcap_{i=0}^{4} W_i = (0, \infty) \cap (1, \infty) \cap (2, \infty) \cap (3, \infty) \cap (4, \infty) = (4, \infty)$

c. $W_0, W_1, W_2, \ldots$ are not mutually disjoint. In fact, $W_{k+1} \subseteq W_k$ for every integer $k \geq 0$.

d. $\displaystyle\bigcup_{i=0}^{n} W_i = (0, \infty)$

e. $\displaystyle\bigcap_{i=0}^{n} W_i = (n, \infty)$

f. $\displaystyle\bigcup_{i=0}^{\infty} W_i = (0, \infty)$

g. $\displaystyle\bigcap_{i=0}^{\infty} W_i = \varnothing$

27. a. No. The element d is in two of the sets.

b. No. None of the sets contains 6.

28. Yes. Every integer is either even or odd, and no integer is both even and odd.

31. a. $A \cap B = \{2\}$, so $\mathcal{P}(A \cap B) = \{\varnothing, \{2\}\}$.

b. $A = \{1, 2\}$, so $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

c. $A \cup B = \{1, 2, 3\}$, so $\mathcal{P}(A \cup B) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

d. $A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$, so $\mathcal{P}(A \times B) = \{\varnothing, \{(1, 2)\}, \{(1, 3)\}, \{(2, 2)\}, \{(2, 3)\}, \{(1, 2), (1, 3)\}, \{(1, 2), (2, 2)\}, \{(1, 2), (2, 3)\}, \{(1, 3), (2, 2)\}, \{(1, 3), (2, 3)\},$

$\{(2, 2), (2, 3)\}, \{(1, 2), (1, 3), (2, 2)\},$
$\{(1, 2), (1, 3), (2, 3)\},$
$\{(1, 2), (2, 2), (2, 3)\}, \{(1, 3), (2, 2), (2, 3)\},$
$\{(1, 2), (1, 3), (2, 2), (2, 3)\}\}$.

32. a. $\mathcal{P}(A \times B) = \{\varnothing, \{(1, u)\}, \{(1, v)\}, \{(1, u), (1, v)\}\}$

33. b. $\mathcal{P}(\mathcal{P}(\varnothing)) = \mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$

34. a. $A_1 \cup (A_2 \times A_3)$
$= \{1\} \cup \{(u, m), (u, n), (v, m), (v, n)\}$
$= \{1, (u, m), (u, n), (v, m), (v, n)\}$

35. a. $A \times (B \cup C) = \{a, b\} \times \{1, 2, 3\}$
$= \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$

b. $(A \times B) \cup (A \times C) = \{(a, 1), (a, 2), (b, 1), (b, 2), (a, 2), (a, 3), (b, 2), (b, 3)\}$
$= \{(a, 1), (a, 2), (b, 1), (b, 2), (a, 3), (b, 3)\}$

36.

i	1	→	→	→	2	→	→	→	3	→	→	4
j		1	2	3	1	2	3	4	1	→	2	
found		no	yes		no		yes		no	yes		
answer	$A \subseteq B$											

SECTION 6.2

1. a. (1) A (2) $B \cup C$
b. (1) $A \cap B$
(2) C
d. (1) $(A \cup B) \cap C$ (2) $A \cup (B \cap C)$

2. a. (1) $A - B$ (2) A (3) A (4) B

3. a. by definition of subset (because $A \subseteq B$)
b. by definition of subset (because $B \subseteq C$)
c. by definition of subset

5. Proof: Suppose A and B are any sets.

Proof that $B - A \subseteq B \cap A^c$: Suppose $x \in B - A$. By definition of set difference, $x \in B$ and $x \notin A$. It follows by definition of complement that $x \in B$ and $x \in A^c$, and so by definition of intersection, $x \in B \cap A^c$. *[Thus $B - A \subseteq B \cap A^c$ by definition of subset.]*

Proof that $B \cap A^c \subseteq B - A$: Suppose $x \in B \cap A^c$. By definition of intersection, $x \in B$ and $x \in A^c$. It follows by definition of complement that $x \in B$ and $x \notin A$, and so by definition of set difference, $x \in B - A$. *[Thus $B \cap A^c \subseteq B - A$ by definition of subset.]*

[Since both subset relations have been proved, $B - A = B \cap A^c$ by definition of set equality.]

6. *Partial answers*
(1) **a.** $(A \cap B) \cup (A \cap C)$ **b.** A **c.** $x \in C$
d. $x \in (A \cap B) \cup (A \cap C)$

7. *Hint:* This is somewhat similar to the proof in Example 6.2.3.

8. Proof: Suppose A and B are any sets.

Proof that $(A \cap B) \cup (A \cap B^c) \subseteq A$: Suppose $x \in (A \cap B) \cup (A \cap B^c)$. *[We must show that $x \in A$.]* By definition of union, $x \in A \cap B$ or $x \in (A \cap B^c)$.

Case 1 ($x \in A \cap B$): In this case x is in A and x is in B, and so, in particular, $x \in A$.

Case 2 ($x \in A \cap B^c$): In this case x is in A and x is not in B, and so, in particular, $x \in A$.

Thus, in either case, $x \in A$ *[as was to be shown].* So $(A \cap B) \cup (A \cap B^c) \subseteq A$ *[by definition of subset].*

Proof that $A \subseteq (A \cap B) \cup (A \cap B^c)$: Suppose $x \in A$. *[We must show that $x \in (A \cap B) \cup (A \cap B^c)$.]* Either $x \in B$ or $x \notin B$.

Case 1 ($x \in B$): In this case we know that x is in A and we are also assuming that x is in B. Hence, by definition of intersection, $x \in A \cap B$.

Case 2 ($x \in A \cap B^c$): In this case we know that x is in A and we are also assuming that x is in B^c. Hence, by definition of intersection, $x \in A \cap B^c$.

Thus, in either case $x \in A \cap B$ or $x \in A \cap B^c$, and so, by definition of union, $x \in (A \cap B) \cup (A \cap B^c)$ *[as was to be shown]. So $A \subseteq (A \cap B) \cup (A \cap B^c)$ [by definition of subset].*

Conclusion: Since both subset relations have been proved it follows by definition of set equality that $(A \cap B) \cup (A \cap B^c) = A$.

9. Partial proof: Suppose A, B, and C are any sets. To show that $(A - B) \cup (C - B) = (A \cup C) - B$, we must show that $(A - B) \cup (C - B) \subseteq (A \cup C) - B$ and that $(A \cup C) - B \subseteq (A - B) \cup (C - B)$.

Proof that $(A - B) \cup (C - B) \subseteq (A \cup C) - B$: Suppose that x is any element in $(A - B) \cup (C - B)$. *[We must show that $x \in (A \cup C) - B$.]* By definition of union, $x \in A - B$ or $x \in C - B$.

Case 1 ($x \in A - B$): Then, by definition of set difference, $x \in A$ and $x \notin B$. Now because $x \in A$, we have that $x \in A \cup C$ by definition of union. Hence $x \in A \cup C$ and $x \notin B$, and so, by definition of set difference, $x \in (A \cup C) - B$.

Case 2 ($x \in C - B$): Then, by definition of set difference, $x \in C$ and $x \notin B$. Now because $x \in C$, we have that $x \in A \cup C$ by definition of union. Hence $x \in A \cup C$ and $x \notin B$, and so, by definition of set difference, $x \in (A \cup C) - B$.

Thus, in both cases, $x \in (A \cup C) - B$ *[as was to be shown].* So $(A - B) \cup (C - B) \subseteq (A \cup C) - B$ *[by definition of subset].* To complete the proof that

$(A - B) \cup (C - B) = (A \cup C) - B$, you must show that $(A \cup C) - B \subseteq (A - B) \cup (C - B)$.

10. Proof: Suppose A, B, and C are any sets.

We will show that $(A \cup B) \cap C \subseteq A \cup (B \cap C)$.

Suppose x is any element $(A \cup B) \cap C$.

By definition of intersection x is in $A \cup B$ and x is in C.

Then by definition of union x is in A or x is in B, and in both cases x is in C. It follows by definition of union that in case x is in A and x is in C, then x is in $A \cup (B \cap C)$ by virtue of being in A. And in case x is in $B \cap C$, then x is in $A \cup (B \cap C)$ by virtue of being in $B \cap C$. Thus in both cases x is in $A \cup (B \cap C)$, which proves that every element in $(A \cup B) \cap C$ is in $A \cup (B \cap C)$.

Hence $(A \cup B) \cap C \subseteq A \cup (B \cap C)$ by definition of subset.

14. Partial proof: Suppose A and B are any sets. We will show that $A \cup (A \cap B) \subseteq A$. Suppose x is any element in $A \cup (A \cap B)$. *[We must show that $x \in A$.]* By definition of union, $x \in A$ or $x \in A \cap B$. In the case where $x \in A$, clearly $x \in A$. In the case where $x \in A \cap B$, $x \in A$ and $x \in B$ (by definition of intersection), and so, in particular, $x \in A$. Hence, in both cases $x \in A$ *[as was to be shown]*. Thus $A \cup (A \cap B) \subseteq A$ by definition of subset.

To complete the proof that $A \cup (A \cap B) = A$, you must show that $A \subseteq A \cup (B \cap A)$.

15. Proof: Let A be any set. *[We must show that $A \cup \varnothing = A$.]*

Proof that $A \cup \varnothing \subseteq A$: Suppose $x \in A \cup \varnothing$. Then $x \in A$ or $x \in \varnothing$ by definition of union. But $x \notin \varnothing$ since $\varnothing$ has no elements. Hence $x \in A$.

Proof that $A \subseteq A \cup \varnothing$: Suppose $x \in A$. Then the statement "$x \in A$ or $x \in \varnothing$" is true. Hence $x \in A \cup \varnothing$ by definition of union. *[Alternatively, $A \subseteq A \cup \varnothing$ by the inclusion in union property.]*

Since $A \cup \varnothing \subseteq A$ and $A \subseteq A \cup \varnothing$, then $A \cup \varnothing = A$ by definition of set equality.

16. Proof: Suppose A, B, and C are any sets such that $A \subseteq B$. Let $x \in A \cap C$. By definition of intersection, $x \in A$ and $x \in C$. Now since $A \subseteq B$ and $x \in A$, then $x \in B$. Hence $x \in B$ and $x \in C$, and so, by definition of intersection, $x \in B \cap C$. *[Thus $A \cap C \subseteq B \cap C$ by definition of subset.]*

19. *Hint:* The proof has the following outline:

Starting point: Suppose A, B, and C are any sets such that $A \subseteq B$ and $A \subseteq C$.

To show: $A \subseteq B \cap C$.

21. Proof: Suppose A, B, and C are arbitrarily chosen sets.

$A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$: Suppose $(x, y) \in A \times (B \cup C)$. *[We must show that $(x, y) \in (A \times B) \cup (A \times C)$.]* Then $x \in A$ and $y \in B \cup C$. By definition of union, this means that $y \in B$ or $y \in C$.

Case 1 ($y \in B$): Then, since $x \in A$, $(x, y) \in A \times B$ by definition of Cartesian product. Hence $(x, y) \in (A \times B) \cup (A \times C)$ by definition of union.

Case 2 ($y \in C$): Then, since $x \in A$, $(x, y) \in A \times C$ by definition of Cartesian product. Hence $(x, y) \in (A \times B) \cup (A \times C)$ by definition of union.

Hence, in either case, $(x, y) \in (A \times B) \cup (A \times C)$ *[as was to be shown]*.

Thus $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ by definition of subset.

$(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$: Suppose $(x, y) \in (A \times B) \cup (A \times C)$. Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$.

Case 1 ($(x, y) \in A \times B$): In this case, $x \in A$ and $y \in B$. Now since $y \in B$ then $y \in B \cup C$ by definition of union. Hence $x \in A$ and $y \in B \cup C$, and so, by definition of Cartesian product, $(x, y) \in A \times (B \cup C)$.

Case 2 ($(x, y) \in A \times C$): In this case $x \in A$ and $y \in C$. Now since $y \in C$, then $y \in B \cup C$ by definition of union. Hence $x \in A$ and $y \in B \cup C$, and so, by definition of Cartesian product, $(x, y) \in A \times (B \cup C)$.

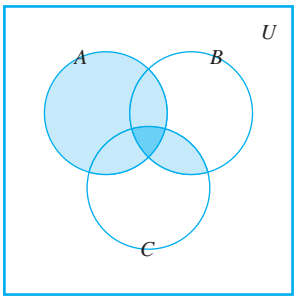
Thus, in either case, $(x, y) \in A \times (B \cup C)$. *[Hence, by definition of subset, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.]*

[Since both subset relations have been proved, we can conclude that $A \times (B \cup C) = (A \times B) \cup (A \times C)$ by definition of set equality.]

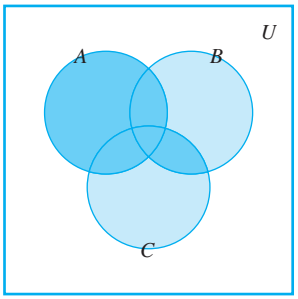
23. There is more than one error in this "proof." The most serious is the misuse of the definition of subset. To say that A is a subset of B means that for every x, **if** $x \in A$ **then** $x \in B$. It does not mean that there exists an element of A that is also an element of B. The second error in the proof occurs in the last sentence. Even if there is an element in A that is in B and an element in B that is in C, it does not follow that there is an element in A that is in C. For instance, suppose $A = \{1, 2\}$, $B = \{2, 3\}$, and $C = \{3, 4\}$. Then there is an element in A that is in B (namely 2) and there is an element in B that is in C (namely, 3), but there is no element in A that is in C.

24. *Hint:* The words "and so $x \notin A \cup B$" do not necessarily follow from "$x \notin A$ or $x \notin B$." Try to think of an example of sets A and B and an element x for which "$x \notin A$ or $x \notin B$" is true and "$x \notin A \cup B$" is false.

26. a.



The shaded region is $A \cup (B \cap C)$.



The most darkly shaded region is $(A \cup B) \cap (A \cup C)$.

27. **(a)** $(A - B) \cap (B - A)$
(b) intersection
(c) $B - A$
(d) B
(e) A
(f) A
(g) $(A - B) \cap (B - A) = \varnothing$

28. Proof by contradiction: Suppose not. That is, suppose there exist sets A and B such that $(A \cap B) \cap (A \cap B^c) \neq \varnothing$. Then there is an element x in $(A \cap B) \cap (A \cap B^c)$. By definition of intersection, $x \in (A \cap B)$ and $x \in (A \cap B^c)$. Applying the definition of intersection again, we have that since $x \in (A \cap B)$, $x \in A$ and $x \in B$, and since $x \in (A \cap B^c)$, $x \in A$ and $x \notin B$. Thus, in particular, $x \in B$ and $x \notin B$, which is a contradiction. It follows that the supposition is false, and so $(A \cap B) \cap (A \cap B^c) = \varnothing$.

30. Proof: Let A be a subset of a universal set U. Suppose $A \cap A^c \neq \varnothing$, that is, suppose there is an element x such that $x \in A \cap A^c$. By definition of intersection, $x \in A$ and $x \in A^c$, and so by definition of complement, $x \in A$ and $x \notin A$. This is a contradiction. *[Hence the supposition is false, and we conclude that $A \cap A^c = \varnothing$.]*

32. Proof: Let A be a set. Suppose $A \times \varnothing \neq \varnothing$. Then there would be an element (x, y) in $A \times \varnothing$. By definition of Cartesian product, $x \in A$ and $y \in \varnothing$. But there are no elements y such that $y \in \varnothing$. Hence there are no elements (x, y) in $A \times \varnothing$, which is a contradiction. *[Thus the supposition is false, and so $A \times \varnothing = \varnothing$.]*

33. Proof: Let A and B be sets such that $A \subseteq B$. *[We must show that $A \cap B^c = \varnothing$.]* Suppose $A \cap B^c \neq \varnothing$; that is, suppose there were an element x such that $x \in A \cap B^c$. Then $x \in A$ and $x \in B^c$ by definition of intersection. So $x \in A$ and $x \notin B$ by definition of complement. But $A \subseteq B$ by hypothesis, and, since $x \in A$, then $x \in B$ by definition of subset. Thus $x \notin B$ and also $x \in B$, which is a contradiction. Hence the supposition that $A \cap B^c \neq \varnothing$ is false, and so $A \cap B^c = \varnothing$.

36. Proof: Let A, B, and C be any sets such that $C \subseteq B - A$. Suppose $A \cap C \neq \varnothing$. Then there is an element x such that $x \in A \cap C$. By definition of intersection, $x \in A$ and $x \in C$. Now since $x \in C$ and $C \subseteq B - A$, then $x \in B$ and $x \notin A$. So $x \in A$ and $x \notin A$, which is a contradiction. Hence the supposition is false, and thus $A \cap C = \varnothing$.

39. a. *Start of proof that*

$A \cup B \subseteq (A - B) \cup (B - A) \cup (A \cap B)$: Given any element x in $A \cup B$, by definition of union x is in at least one of A and B. Thus x satisfies exactly one of the following three conditions:

(1) $x \in A$ and $x \notin B$ (x is in A only)
(2) $x \in B$ and $x \notin A$ (x is in B only)
(3) $x \in A$ and $x \in B$ (x is in both A and B)

b. To show that $(A - B)$, $(B - A)$, and $(A \cap B)$ are mutually disjoint, we must show that the intersection of any two of them is the empty set. Now, by definition of set difference and set intersection, saying that $x \in A - B$ means that (1) $x \in A$ and $x \notin B$, saying that $x \in B - A$ means that (2) $x \in B$ and $x \notin A$, and saying that $x \in A \cap B$ means that (3) $x \in A$ and $x \in B$. Conditions (1)–(3) are mutually exclusive: no two of them can be satisfied at the same time. Thus no element can be in the intersection of any two of the sets, and, therefore, the intersection of any two of the sets is the empty set. Hence, $(A - B)$, $(B - A)$, and $(A \cap B)$ are mutually disjoint.

40. Suppose that n is any positive integer and that A and B_1, B_2, B_3, . . . , B_n are any sets.

Proof that $A \cap \left(\bigcup_{i=1}^{n} B_i\right) \subseteq \bigcup_{i=1}^{n} (A \cap B_i)$***:***

Suppose x is any element in $A \cap \left(\bigcup_{i=1}^{n} B_i\right)$. *[We must show that* $x \in \bigcup_{i=1}^{n} (A \cap B_i)$*.]* By definition of intersection,

$x \in A$ and $x \in \bigcup_{i=1}^{n} B_i$. Since $x \in \bigcup_{i=1}^{n} B_i$, the definition of general union implies that $x \in B_i$ for some $i = 1, 2, \ldots, n$, and so, since $x \in A$, the definition of intersection implies that $x \in A \cap B_i$. Thus, by definition of general union, $x \in \bigcup_{i=1}^{n} (A \cap B_i)$ *[as was to be shown].*

Proof that $\bigcup_{i=1}^{n} (A \cap B_i) \subseteq A \cap \left(\bigcup_{i=1}^{n} B_i \right)$***:***

Suppose x is any element in $\bigcup_{i=1}^{n} (A \cap B_i)$. *[We must show that* $x \in A \cap \left(\bigcup_{i=1}^{n} B_i \right)$*.]* By definition of general union, $x \in A \cap B_i$ for some $i = 1, 2, \ldots, n$. Thus, by definition of intersection, $x \in A$ and $x \in B_i$. Since $x \in B_i$ for some $i = 1, 2, \ldots, n$, then by definition of general union, $x \in \bigcup_{i=1}^{n} B_i$.

Thus we have that $x \in A$ and $x \in \bigcup_{i=1}^{n} B_i$, and so, by definition of intersection, $x \in A \cap \left(\bigcup_{i=1}^{n} B_i \right)$ *[as was to be shown].*

Conclusion: Since both subset relations have been proved, it follows by definition of set equality that

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \cap B_i).$$

41. *Proof sketch:* If $x \in \bigcup_{i=1}^{n} (A_i - B)$, then $x \in A_i - B$ for some $i = 1, 2, \ldots, n$, and so, (1) for some $i = 1, 2, \ldots, n$, $x \in A_i$ (which implies that $x \in \left(\bigcup_{i=1}^{n} A_i \right)$) and (2) $x \notin B$. Conversely, if $x \in \left(\bigcup_{i=1}^{n} A_i \right) - B$, then $x \in \left(\bigcup_{i=1}^{n} A_i \right)$ and $x \notin B$, and so, by definition of general union, $x \in A_i$ for some $i = 1, 2, \ldots, n$, and $x \notin B$. This implies that there is an integer i such that $x \in A_i - B$, and thus that $x \in \bigcup_{i=1}^{n} (A_i - B)$.

43. Suppose that n is any positive integer and that A and B_1, B_2, B_3, . . . , B_n are any sets.

Proof that $\bigcup_{i=1}^{n} (A \times B_i) \subseteq A \times \left(\bigcup_{i=1}^{n} B_i \right)$***:***

Suppose (x, y) is any element in $\bigcup_{i=1}^{n} (A \times B_i)$. *[We must show that* $(x, y) \in A \times \left(\bigcup_{i=1}^{n} B_i \right)$*.]* By definition of general union, $(x, y) \in A \times B_i$ for some $i = 1, 2, \ldots, n$. By definition of Cartesian product, this implies that (1) $x \in A$ and (2) $y \in B_i$ for some $i = 1, 2, \ldots, n$. By definition of general union, (2) implies that $y \in \bigcup_{i=1}^{n} B_i$. Thus $x \in A$ and $y \in \bigcup_{i=1}^{n} B_i$, and so by definition of Cartesian product, $(x, y) \in A \times \left(\bigcup_{i=1}^{n} B_i \right)$ *[as was to be shown].*

Proof that $A \times \left(\bigcup_{i=1}^{n} B_i \right) \subseteq \bigcup_{i=1}^{n} (A \times B_i)$***:***

Suppose (x, y) is any element in $A \times \left(\bigcup_{i=1}^{n} B_i \right)$. *[We must show that* $(x, y) \in \bigcup_{i=1}^{n} (A \times B_i)$*.]* By definition of Cartesian product, (1) $x \in A$ and (2) $y \in \bigcup_{i=1}^{n} B_i$. By definition of general union, (2) implies that $y \in B_i$ for some $i = 1, 2, \ldots, n$. Thus $x \in A$ and $y \in B_i$ for some $i = 1, 2, \ldots, n$, and so, by definition of Cartesian product, $(x, y) \in A \times B_i$ for some $i = 1, 2, \ldots, n$. It follows from the definition of general union that $(x, y) \in \bigcup_{i=1}^{n} (A \times B_i)$ *[as was to be shown].*

Conclusion: Since both subset relations have been proved, it follows by definition of set equality that $\bigcup_{i=1}^{n} (A \times B_i) = A \times \left(\bigcup_{i=1}^{n} B_i \right)$.

SECTION 6.3

1. Counterexample: A, B, and C can be any sets where A has an element that is not in C. For instance, let $A = \{1, 2\}$, $B = \{2\}$, and $C = \{2\}$. Then $(A \cup B) \cap C = (\{1, 2\} \cup \{2\}) \cap \{2\} = \{1, 2\} \cap \{2\} = \{2\}$, and $A \cup (B \cap C) = \{1, 2\} \cup (\{2\} \cap \{2\}) = \{1, 2\} \cup \{2\} = \{1, 2\}$. Thus $1 \in A \cup (B \cap C)$ but $1 \notin (A \cup B) \cap C$, and hence $(A \cup B) \cap C \neq A \cup (B \cap C)$ by definition of subset.

3. Counterexample: A, B, and C can be any sets where $A \subseteq C$ and B contains at least one element that is not in either A or C. For instance, let $A = \{1\}$, $B = \{2\}$, and $C = \{1, 3\}$. Then $A \not\subseteq B$ and $B \not\subseteq C$ but $A \subseteq C$.

5. False. Counterexample: A, B, and C can be any sets where all three sets have an element in common or where A and C have a common element that is not in B. For instance, let $A = \{1, 2, 3\}$, $B = \{2, 3\}$, and $C = \{3\}$. Then $B - C = \{2\}$, and so $A - (B - C) = \{1, 2, 3\} - \{2\} = \{1, 3\}$.

On the other hand, $A - B = \{1, 2, 3\} - \{2, 3\} = \{1\}$, and so $(A - B) - C = \{1\} - \{3\} = \{1\}$. Since $\{1, 3\} \neq \{1\}$, $A - (B - C) \neq (A - B) - C$.

6. True. Proof: Let A and B be any sets.

Proof that $\boldsymbol{A \cap (A \cup B) \subseteq A}$***:*** Suppose $x \in A \cap (A \cup B)$. By definition of intersection, $x \in A$ and $x \in A \cup B$. In particular, $x \in A$. Thus, by definition of subset, $A \cap (A \cup B) \subseteq A$.

Proof that $\boldsymbol{A \subseteq A \cap (A \cup B)}$***:*** Suppose $x \in A$. Then by definition of union, $x \in A \cup B$. Hence $x \in A$ and $x \in A \cup B$, and so, by definition of intersection $x \in A \cap (A \cup B)$. Thus, by definition of subset, $A \subseteq A \cap (A \cup B)$.

Because both $A \cap (A \cup B) \subseteq A$ and $A \subseteq A \cap (A \cup B)$ have been proved, we conclude that $A \cap (A \cup B) = A$.

9. True. Proof: Suppose A, B, and C are any sets such that $A \subseteq C$ and $B \subseteq C$. Let $x \in A \cup B$. By definition of union, $x \in A$ or $x \in B$. But if $x \in A$ then $x \in C$ (because $A \subseteq C$), and if $x \in B$ then $x \in C$ (because $B \subseteq C$). Hence, in either case, $x \in C$. *[So, by definition of subset,* $A \cup B \subseteq C$*.]*

11. *Hint:* The statement is false. Consider sets U, A, B, and C as follows: $U = \{1, 2, 3, 4\}$, $A = \{1, 2\}$, $B = \{1, 2, 3\}$, and $C = \{2\}$.

12. *Hint:* The statement is true. Observe that if $x \in A \cap (B - C)$, then $x \notin C$, and so $x \notin A \cap C$. Conversely, if $x \in (A \cap B) - (A \cap C)$, then $x \notin A \cap C$, and so, in particular, $x \notin C$.

14. *Hint:* The statement is true. *Sketch of part of proof:* Suppose $x \in A$. *[We must show that* $x \in B$*.]* Either $x \in C$ or $x \notin C$. In case $x \in C$, make use of the fact that $A \cap C \subseteq B \cap C$ to show that $x \in B$. In case $x \notin C$, make use of the fact that $A \cup C \subseteq B \cup C$ to show that $x \in B$.

15. *Hint:* The statement is false.

17. True. Proof: Suppose A and B are any sets with $A \subseteq B$. *[We must show that* $\mathcal{P}(A) \subseteq \mathcal{P}(B)$*.]* So suppose $X \in \mathcal{P}(A)$. Then $X \subseteq A$ by definition of power set. And because $A \subseteq B$, we also have that $X \subseteq B$ by the transitive property for subsets. Thus, by definition of power set, $X \in \mathcal{P}(B)$. This proves that for all X, if $X \in \mathcal{P}(A)$ then $X \in \mathcal{P}(B)$, and so $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ *[as was to be shown].*

18. False. Counterexample: For any sets A and B, the only sets in $\mathcal{P}(A) \cup \mathcal{P}(B)$ are subsets of either A or B, whereas a set in $\mathcal{P}(A \cup B)$ can contain elements from both A and B. Thus, if at least one of A or B contains elements that are not in the other set, $\mathcal{P}(A) \cup \mathcal{P}(B)$ and $\mathcal{P}(A \cup B)$ will not be equal. For instance, let $A = \{1\}$ and $B = \{2\}$. Then $\{1, 2\} \in \mathcal{P}(A \cup B)$ but $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

19. *Hint:* The statement is true. To prove it, suppose A and B are any sets, and suppose $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Note that if $X \subseteq A$, then $X \subseteq A \cup B$, and so $X \in \mathcal{P}(A \cup B)$.

22. a. *Statement:* $\forall$ set S, $\exists$ a set T such that $S \cap T = \varnothing$.

Negation: $\exists$ a set S such that $\forall$ set T, $S \cap T \neq \varnothing$.

The statement is true. Given any set S, take $T = S^c$.

Then $S \cap T = S \cap S^c = \varnothing$ by the complement law for $\cap$. Alternatively, T could be taken to be $\varnothing$.

23. *Hint:* $S_0 = \{\varnothing\}$, $S_1 = \{\{a\}, \{b\}, \{c\}\}$

24. a. $S_1 = \{\varnothing, \{t\}, \{u\}, \{v\}, \{t, u\}, \{t, v\}, \{u, v\}, \{t, u, v\}\}$

b. $S_2 = \{\{w\}, \{t, w\}, \{u, w\}, \{v, w\}, \{t, u, w\}, \{t, v, w\}, \{u, v, w\}, \{t, u, v, w\}\}$

c. Yes

25. *Hint:* The proof uses the same basic idea as the proof of Theorem 6.3.1. In this case let $P(n)$ be the sentence "If a set S has n elements, the number of subsets of S with an even number of elements equals the number of subsets of S with an odd number of elements."

26. *Hint:* Use mathematical induction. In the inductive step, you will consider the set of all nonempty subsets of $\{2, \ldots, k\}$ and the set of all nonempty subsets of $\{2, \ldots, k+1\}$. Any subset of $\{2, \ldots, k+1\}$ either contains $k+1$ or does not contain $k+1$. Thus

$$\begin{bmatrix}\text{the sum of all products}\\ \text{of elements of nonempty}\\ \text{subsets of } \{2, \ldots, k+1\}\end{bmatrix} = \begin{bmatrix}\text{the sum of all products}\\ \text{of elements of nonempty}\\ \text{subsets of } \{2, \ldots, k+1\}\\ \text{that do not contain } k+1\end{bmatrix} + \begin{bmatrix}\text{the sum of all products}\\ \text{of elements of nonempty}\\ \text{subsets of } \{2, \ldots, k+1\}\\ \text{that contain } k+1\end{bmatrix}$$

Now any subset of $\{2, \ldots, k+1\}$ that does not contain $k+1$ is a subset of $\{2, \ldots, k\}$. And any subset of $\{2, \ldots, k+1\}$ that contains $k+1$ is the union of a subset of $\{2, \ldots, k\}$ and $\{k+1\}$.

27. a. commutative law for $\cap$

b. distributive law

c. commutative law for $\cap$

28. Partial answer:

a. set difference law

b. set difference law

c. commutative law for $\cap$

d. De Morgan's law

29. *Hint:* Remember to use the properties in Theorem 6.2.2 exactly as they are written. For example, the distributive law does not state that for all sets A, B, and C, $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

30. Proof: Let sets A, B, and C be given. Then

$(A \cap B) \cup C$

$= C \cup (A \cap B)$ by the commutative law for $\cup$

$= (C \cup A) \cap (C \cup B)$ by the distributive law

$= (A \cup C) \cap (B \cup C)$ by the commutative law for $\cup$.

31. Proof: Suppose A and B are sets. Then

$A \cup (B - A)$

$= A \cup (B \cap A^c)$ by the set difference law

$= (A \cup B) \cap (A \cup A^c)$ by the distributive law

$= (A \cup B) \cap U$ by the complement law for $\cup$

$= A \cup B$ by the identity law for $\cap$.

36. Proof: Let A and B be any sets. Then

$((A^c \cup B^c) - A)^c$

$= ((A^c \cup B^c) \cap A^c)^c$ by the set difference law

$= (A^c \cup B^c)^c \cup (A^c)^c$ by De Morgan's law

$= ((A^c)^c \cap (B^c)^c) \cup (A^c)^c$ by De Morgan's law

$= (A \cap B) \cup A$ by the double complement law

$= A \cup (A \cap B)$ by the commutative law for $\cup$

$= A$ by the absorption law.

39. Partial proof: Let A and B be any sets. Then

$(A - B) \cup (B - A)$

$= (A \cap B^c) \cup (B \cap A^c)$ by the set difference law

$= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c)]$ by the distributive law

$= [(B \cup (A \cap B^c)] \cap [A^c \cup (A \cap B^c)]$ by the commutative law for $\cup$

$= [(B \cup A) \cap (B \cup B^c)] \cap [(A^c \cup A) \cap (A^c \cup B^c)]$ by the distributive law

$= [(A \cup B) \cap (B \cup B^c)] \cap [(A \cup A^c) \cap (A^c \cup B^c)]$ by the commutative law for $\cup$.

41. *Hint:* The answer is $\varnothing$.

44. a. Proof (by contradiction): Suppose not. That is, suppose there exist sets A and B such that $A - B$ and B are not disjoint. Then $(A - B) \cap B \neq \varnothing$, which means there is an element x in $(A - B) \cap B$. By definition of intersection, $x \in A - B$ and $x \in B$, and by definition of set difference, $x \in A$ and $x \notin B$. Hence $x \in B$ and $x \notin B$, which is a contradiction. Thus the supposition is false, and so $A - B$ and B are disjoint.

b. Let A and B be any sets. Then

$(A - B) \cap B$

$= (A \cap B^c) \cap B$ by the set difference law

$= A \cap (B^c \cap B)$ by the associative law for $\cap$

$= A \cap (B \cap B^c)$ by the commutative law for $\cap$

$= A \cap \varnothing$ by the complement law for $\cap$

$= \varnothing$ by the universal bound law for $\cap$.

Thus $A - B$ and B are disjoint.

46. a. $A \Delta B = (A - B) \cup (B - A) = \{1, 2\} \cup \{5, 6\} = \{1, 2, 5, 6\}$

47. Proof: Let A and B be any subsets of a universal set. By definition of Δ, showing that $A \Delta B = B \Delta A$ is equivalent to showing that $(A - B) \cup (B - A) = (B - A) \cup (A - B)$. This follows immediately from the commutative law for $\cup$.

48. Proof: Let A be any subset of a universal set. Then

$A \Delta \varnothing$

$= (A - \varnothing) \cup (\varnothing - A)$ by definition of Δ

$= (A \cap \varnothing^c) \cup (\varnothing \cap A^c)$ by the set difference law

$= (A \cap U) \cup (A^c \cap \varnothing)$ by the complement of $\cup$ law and the commutative law for $\cap$

$= A \cup \varnothing$ by the identity law for $\cap$ and the universal bound law for $\cap$

$= A$ by the identity law for $\cup$.

51. *Hint:* First show that for any sets A and B and for any element x,

$x \in A \Delta B \Leftrightarrow (x \in A$ and $x \notin B)$ or $(x \in B$ and $x \notin A)$

and

$x \notin A \Delta B \Leftrightarrow (x \notin A$ and $x \notin B)$ or $(x \in B$ and $x \in A)$.

52. Same hint as for exercise 51.

53. *Start of proof:* Suppose A and B are any subsets of a universal set U. By the universal bound law for union, $B \cup U = U$, and so, by the commutative law for union, $U \cup B = U$. Take the intersection of both sides of the equation with A.

SECTION 6.4

1. a. because 1 is an identity for $\cdot$

b. by the complement law for $+$

c. by the distributive law for $+$ over $\cdot$

d. by the complement law for $\cdot$

e. because 0 is an identity for $+$

4. Proof: For every a in B,

$a \cdot 0 = a \cdot (a \cdot \bar{a})$ by the complement law for $\cdot$

$= (a \cdot a) \cdot \bar{a}$ by the associative law for $\cdot$

$= a \cdot \bar{a}$ by exercise 1

$= 0$ by the complement law for $\cdot$.

5. a. Proof: $0 \cdot 1 = 0$ because 1 is an identity for $\cdot$, and $0 + 1 = 1 + 0 = 1$ because $+$ is commutative and 0 is an identity for $+$. Thus, by the uniqueness of the complement law, $\bar{0} = 1$.

6. Proof: Suppose 0 and $0'$ are elements of B both of which are identities for $+$. Then both 0 and $0'$ satisfy the identity, complement, and universal bound laws. *[We will show that* $0 = 0'$*.]* By the identity law for $+$, for every $a \in B$,

$a + 0 = a$ (*) and $a + 0' = a$ (**).

It follows that

$0' = 0' + 0$ by (*) with $a = 0'$

$= 0 + 0'$ by the commutative law for $+$

$= 0$ by (**) with $a = 0$.

[This is what was to be shown.]

7. *Hint:* Suppose 1 and $1'$ are elements of B both of which are identities for $\cdot$. Then for every $a \in B$, by the identity law for $\cdot$, $a \cdot 1 = a$ and $a \cdot 1' = a$. It follows that $a \cdot 1 = a \cdot 1'$, and thus $\bar{a} + a \cdot 1 = \bar{a} + a \cdot 1'$, and so forth.

8. Proof: Suppose B is a Boolean algebra and a and b are any elements of B. We first prove that $(a \cdot b) + (\bar{a} + \bar{b}) = 1$.

$a \cdot b + (\bar{a} + \bar{b})$

$= ((a \cdot b) \cdot \bar{a}) + ((a \cdot b) \cdot \bar{b})$
by the commutative law for $+$

$= ((b \cdot a) \cdot a) \cdot (\bar{a} \cdot (\bar{b} \cdot b))$
by the distributive law of $+$ over $\cdot$

$= ((\bar{b} + \bar{a}) + a) \cdot (\bar{a} + (\bar{b} + b))$
by the commutative and associative laws for $+$

$= (\bar{b} + (\bar{a} + a)) \cdot (\bar{a} + (b + \bar{b}))$
by the associative and commutative laws for $+$

$= (\bar{b} + (a + \bar{a})) \cdot (\bar{a} + 1)$
by the commutative and complement laws for $+$

$= (\bar{b} + 1) \cdot 1$ by the universal bound laws for $+$

$= 1 \cdot 1$ by the universal bound law for $+$

$= 1$ by the identity law for $\cdot$.

Next we prove that $(a \cdot b) \cdot (\bar{a} + \bar{b}) = 0$.

$(a \cdot b) \cdot (\bar{a} + \bar{b})$

$= ((a \cdot b) \cdot \bar{a}) + ((a \cdot b) \cdot \bar{b})$
by the distributive law of $\cdot$ over $+$

$= ((b \cdot a) \cdot \bar{a}) + (a \cdot (b \cdot \bar{b}))$
by the commutative and associative laws for $\cdot$

$= (b \cdot (a \cdot \bar{a})) + (a \cdot 0)$
by the associative and complement laws for $\cdot$

$= (b \cdot 0) + 0$
by the complement and universal bound laws for $\cdot$

$= 0 + 0$ by the universal bound law for $\cdot$

$= 0$ by the identity law for $+$.

Because both $(a \cdot b) + (\bar{a} + \bar{b}) = 1$ and $(a \cdot b) \cdot (\bar{a} + \bar{b}) = 0$, it follows, by the uniqueness of the complement law, that $\overline{a \cdot b} = \bar{a} + \bar{b}$.

10. *Hint:* One way to prove the statement is to use the result of exercise 3. Some stages in the proof are the following:

$$y = (y + x) \cdot y = \cdots = (x \cdot y) + (z \cdot y) = \cdots$$
$$= z \cdot (x + y) = \cdots = z.$$

11. a. (i) Because S has only two distinct elements, 0 and 1, we only need to check that $0 + 1 = 1 + 0$. This is true because both sums equal 1.

(v) *Partial answer:* Show that for all a, b, and c in B, $a + (b \cdot c) = (a + b) \cdot (a + b)$.

$0 + (0 \cdot 0) = 0 + 0 = 0$ and $(0 + 0) \cdot (0 + 0)$
$= 0 \cdot 0 = 0$ $[a = b = c = 0]$

$0 + (0 \cdot 1) = 0 + 0 = 0$ and $(0 + 0) \cdot (0 + 1)$
$= 0 \cdot 1 = 0$ $[a = b = 0, c = 1]$

$0 + (1 \cdot 0) = 0 + 0 = 0$ and $(0 + 1) \cdot (0 + 0)$
$= 1 \cdot 0 = 0$ $[a = c = 0, b = 1]$

$0 + (1 \cdot 1) = 0 + 1 = 1$ and $(0 + 1) \cdot (0 + 1)$
$= 1 \cdot 1 = 1$ $[a = 0, b = c = 1]$

b. *Hint:* Verify that $0 + x = x$ and that $1 \cdot x = x$ for every $x \in S$.

12. Proof: Suppose a is any element of a Boolean algebra B.

$a + 1 = (a + 1) \cdot 1$ because 1 is an identity for $\cdot$

$= (a + 1) \cdot (a + \bar{a})$ by the complement law for $+$

$= a + 1 \cdot \bar{a}$ by the distributive law for $+$ over $\cdot$

$= a + \bar{a} \cdot 1$ by the commutative law for $\cdot$

$= a + \bar{a}$ because 1 is an identity for $\cdot$

$= 1$ by the complement law for $+$.

13. *Start of proof:* Suppose a and b are any elements of a Boolean algebra B.

$a \cdot b + a = a \cdot b + a \cdot 1$ because 1 is an identity for $\cdot$

15. For part (1), show that both sides of the equation equal a. For part (2), show that both sides of the equation equal $\bar{a} \cdot (b + c)$.

16. The sentence is not a statement because it is both true and false. If the sentence were true, then because it declares itself to be false, the sentence would be false. Therefore, the sentence is not true. On the other hand,

if the sentence were false, then it would be false that "This sentence is false," and so the sentence would be true. Consequently, the sentence is false. It follows that the sentence is both true and false.

17. This sentence is a statement because it is true. Recall that the only way for an if-then statement to be false is for the hypothesis to be true and the conclusion false. In this case the hypothesis is not true. So regardless of what the conclusion states, the sentence is true. (This is an example of a statement that is vacuously true, or true by default.)

20. This sentence is not a statement because it is both true and false. If the sentence is true, then, by definition of an *or* statement, either the sentence is false or $1 + 1 = 3$. But $1 + 1 \neq 3$, and so the sentence is false. On the other hand, if the sentence is false, then (by DeMorgan's law) both of the following must be true: "This sentence is false" and "$1 + 1 = 3$." But it is not true that $1 + 1 = 3$. So it is impossible for the sentence to be false and hence the sentence is true. Consequently, the sentence is both true and false.

23. *Hint:* Suppose that apart from statement (ii), all of Nixon's other assertions about Watergate are evenly split between true and false.

24. No. Suppose there exists a computer program P that has as output a list of all computer programs that do not list themselves in their output. If P lists itself as output, then it would be on the output list of P, which consists of all computer programs that do not list themselves in their output. Hence P would not list itself as output. But if P does not list itself as output, then P would be a member of the list of all computer programs that do not list themselves in their output, and this list is exactly the output of P. Hence P would list itself as output. This analysis shows that the assumption of the existence of such a program P is contradictory, and so no such program exists.

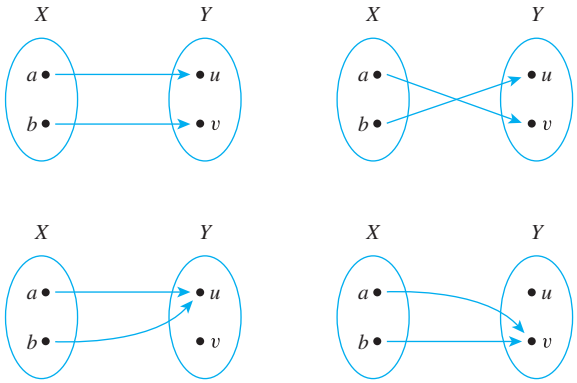
28. *Hint:* Show that any algorithm that solves the printing problem can be adapted to produce an algorithm that solves the halting problem.

SECTION 7.1

1. a. domain of $f = \{1, 3, 5\}$, co-domain of $f = \{s, t, u, v\}$
b. $f(1) = v, f(3) = s, f(5) = v$
c. range of $f = \{s, v\}$
d. yes, no
e. inverse image of $s = \{3\}$, inverse image of $u = \varnothing$, inverse image of $v = \{1, 5\}$
f. $\{(1, v), (3, s), (5, v)\}$

3. a. True. The definition of function says that for any input there is one and only one output, so if two inputs are equal, their outputs must also be equal.
c. True. The definition of function does not prohibit this occurrence.

4. a. There are four functions from X to Y as shown below.



5. a. $I_Z(e) = e$
b. $I_Z\left(b_i^{jk}\right) = b_i^{jk}$

6. a. The sequence is given by the function $f: \mathbf{Z}^{nonneg} \to \mathbf{R}$ defined by the rule

$$f(n) = \frac{(-1)^n}{2n+1} \quad \text{for each nonnegative integer } n.$$

7. a. $F(\{1, 3, 4\}) = 1$ *[because* $\{1, 3, 4\}$ *has an odd number of elements]*
c. $F(\{2, 3\}) = 0$ *[because* $\{2, 3\}$ *has an even number of elements]*

8. a. $F(0) = (0^3 + 2 \cdot 0 + 4) \bmod 5 = 4 \bmod 5 = 4$
b. $F(1) = (1^3 + 2 \cdot 1 + 4) \bmod 5 = 7 \bmod 5 = 2$

9. a. $S(1) = 1$ **b.** $S(15) = 1 + 3 + 5 + 15 = 24$
c. $S(17) = 1 + 17 = 18$

10. a. $T(1) = \{1\}$ **b.** $T(15) = \{1, 3, 5, 15\}$
c. $T(17) = \{1, 17\}$

11. a. $F(4, 4) = (2 \cdot 4 + 1, 3 \cdot 4 - 2) = (9, 10)$
b. $F(2, 1) = (2 \cdot 2 + 1, 3 \cdot 1 - 2) = (5, 1)$

12. a. $G(4, 4) = ((2 \cdot 4 + 1) \bmod 5, (3 \cdot 4 - 2) \bmod 5) = (9 \bmod 5, 10 \bmod 5) = (4, 0)$
b. $G(2, 1) = ((2 \cdot 2 + 1) \bmod 5, (3 \cdot 1 - 2) \bmod 5) = (5 \bmod 5, 1 \bmod 5) = (0, 1)$

13.

x	$f(x)$	$g(x)$
0	$4^2 \bmod 5 = 1$	$(0^2 + 3 \cdot 0 + 1) \bmod 5 = 1$
1	$5^2 \bmod 5 = 0$	$(1^2 + 3 \cdot 1 + 1) \bmod 5 = 0$
2	$6^2 \bmod 5 = 1$	$(2^2 + 3 \cdot 2 + 1) \bmod 5 = 1$
3	$7^2 \bmod 5 = 4$	$(3^2 + 3 \cdot 3 + 1) \bmod 5 = 4$
4	$8^2 \bmod 5 = 4$	$(4^2 + 3 \cdot 4 + 1) \bmod 5 = 4$

The table shows that $f(x) = g(x)$ for every x in J_5. Thus, by definition of equality of functions, $f = g$.

15. $F \cdot G$ and $G \cdot F$ are equal because for every real number x,

$$\begin{aligned}(F\cdot G)(x) &= F(x)\cdot G(x) && \text{by definition of } F\cdot G\\ &= G(x)\cdot F(x) && \text{by the commutative law for multiplication of real numbers}\\ &= (G\cdot F)(x) && \text{by definition of } G\cdot F.\end{aligned}$$

17. a. $2^3 = 8$ **c.** $4^1 = 4$

18. a. $\log_3 81 = 4$ because $3^4 = 81$

c. $\log_3\left(\frac{1}{27}\right) = -3$ because $3^{-3} = \frac{1}{27}$

19. Let b be any positive real number with $b \neq 1$. Since $b^1 = b$, then $\log_b b = 1$ by definition of logarithm.

21. Proof: Suppose b and u are any positive real numbers with $b \neq 1$. *[We must show that* $\log_b\left(\frac{1}{u}\right) = -\log_b(u)$*.]* Let $v = \log_b\left(\frac{1}{u}\right)$. By definition of logarithm, $b^v = \frac{1}{u}$. Multiplying both sides by u and dividing by b^v gives $u = b^{-v}$, and thus, by definition of logarithm, $-v = \log_b(u)$. When both sides of this equation are multiplied by -1, the result is $v = -\log_b(u)$. Therefore, $\log_b\left(\frac{1}{u}\right) = -\log_b(u)$ because both expressions equal v. *[This is what was to be shown.]*

22. *Hint:* Use a proof by contradiction. Suppose $\log_3 7$ is rational. Then $\log_3 7 = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

Apply the definition of logarithm to rewrite $\log_3 7 = \frac{a}{b}$ in exponential form.

23. Suppose b and y are positive real numbers with $\log_b y = 3$.

By definition of logarithm, this implies that $b^3 = y$. Then

$$y = b^3 = \frac{1}{\frac{1}{b^3}} = \frac{1}{\left(\frac{1}{b}\right)^3} = \left(\frac{1}{b}\right)^{-3}.$$

Thus, by definition of logarithm (with base $1/b$), $\log_{1/b}(y) = -3$.

25. a. $p_1(2, y) = 2$, $p_1(5, x) = 5$, range of $p_1 = \{2, 3, 5\}$

26. a. $mod(67, 10) = 7$ and $div(67, 10) = 6$ since $67 = 10 \cdot 6 + 7$.

27. $f(aba) = 0$ *[because there are no b's to the left of the left-most a in aba]*

$f(bbab) = 2$ *[because there are two b's to the left of the left-most a in bbab]*

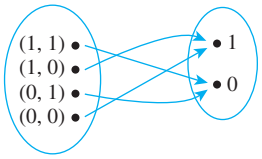
$f(b) = 0$ *[because the string b contains no a's]*

range of $f = Z^{nonneg}$

28. a. $E(0110) = 000111111000$ and $D(111111000111) = 1101$

29. a. $H(10101, 00011) = 3$

30. a.



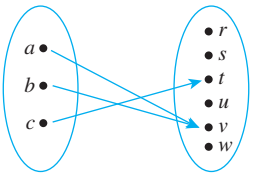
32. a. $f(1, 1, 1) = (4\cdot 1 + 3\cdot 1 + 2\cdot 1)\ mod\ 2$
$= 9\ mod\ 2 = 1$

$f(0, 0, 1) = (4\cdot 0 + 3\cdot 0 + 2\cdot 1)\ mod\ 2$
$= 2\ mod\ 2 = 0$

33. If g were well defined, then $g(1/2) = g(2/4)$ because $1/2 = 2/4$. However, $g(1/2) = 1 - 2 = -1$ and $g(2/4) = 2 - 4 = -2$. Since $-1 \neq -2$, $g(1/2) \neq g(2/4)$. Thus g is not well defined.

35. Student B is correct. If R were well defined, then $R(3)$ would have a uniquely determined value. However, on the one hand, $R(3) = 2$ because $(3\cdot 2)\ mod\ 5 = 1$, and, on the other hand, $R(3) = 7$ because $(3\cdot 7)\ mod\ 5 = 1$. Hence $R(3)$ does not have a uniquely determined value, and so R is not well defined.

38. a.

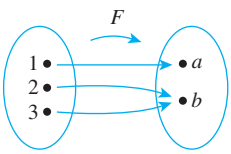


b. $f(A) = \{v\}$, $f(X) = \{t, v\}$, $f^{-1}(C) = \{c\}$, $f^{-1}(D) = \{a, b\}$, $f^{-1}(E) = \varnothing$, $f^{-1}(Y) = \{a, b, c\} = X$

40. *Partial answer:* ***(i)*** $y \in F(A)$ or $y \in F(B)$ ***(ii)*** some ***(iii)*** $A \cup B$ ***(iv)*** $F(A \cup B)$

41. The statement is true. Proof: Let F be a function from X to Y, and suppose $A \subseteq X$, $B \subseteq X$, and $A \subseteq B$. Let $y \in F(A)$. *[We must show that* $y \in F(B)$*.]* By definition of image of a set, $y = F(x)$ for some $x \in A$. Thus since $A \subseteq B$, $x \in B$, and so $y = F(x)$ for some $x \in B$. Hence $y \in F(B)$ *[as was to be shown].*

43. The statement is false. Counterexample: Let $X = \{1, 2, 3\}$, let $Y = \{a, b\}$, and define a function F: $X \to Y$ by the arrow diagram shown below.



Let $A = \{1, 2\}$ and $B = \{1, 3\}$. Then $F(A) = \{a, b\} = F(B)$, and so $F(A) \cap F(B) = \{a, b\}$. But $F(A \cap B) = F(\{1\}) = \{a\} \neq \{a, b\}$. And so $F(A) \cap F(B) \not\subseteq F(A \cap B)$.

(This is just one of many possible counterexamples.)

45. The statement is true. Proof: Let F be a function from a set X to a set Y, and suppose $C \subseteq Y$, $D \subseteq Y$, and $C \subseteq D$. *[We must show that $F^{-1}(C) \subseteq F^{-1}(D)$.]* Suppose $x \in F^{-1}(C)$. Then $F(x) \in C$. Since $C \subseteq D$, $F(x) \in D$ also. Hence, by definition of inverse image, $x \in F^{-1}(D)$. *[So $F^{-1}(C) \subseteq F^{-1}(D)$.]*

46. *Hint:* $x \in F^{-1}(C \cup D) \Leftrightarrow F(x) \in C \cup D \Leftrightarrow F(x) \in C$ or $F(x) \in D$

51. **a.** $\phi(15) = 8$ *[because* 1, 2, 4, 7, 8, 11, 13, *and* 14 *have no common factors with* 15 *other than* ± 1*]*

b. $\phi(2) = 1$ *[because the only positive integer less than or equal to* 2 *having no common factors with* 2 *other than* ± 1 *is* 1*]*

c. $\phi(5) = 4$ *[because* 1, 2, 3, *and* 4 *have no common factors with* 5 *other than* ± 1*]*

52. Proof: Let p be any prime number and n any integer with $n \geq 1$. There are p^{n-1} positive integers less than or equal to p^n that have a common factor other than ± 1 with p^n—namely, $p, 2p, 3p, \ldots, (p^{n-1})p$. Hence, there are $p^n - p^{n-1}$ positive integers less than or equal to p^n that do not have a common factor with p^n except for ± 1.

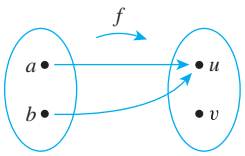
53. *Hint:* Use the result of exercise 52 with $p = 2$.

SECTION 7.2

1. The second statement is the contrapositive of the first.

2. **a.** most

3. *Hint:* One counterexample is given and explained below. Give a different counterexample and accompany it with an explanation. Counterexample: Consider the function defined by the following arrow diagram:



Observe that a is sent to exactly one element of Y, namely, u, and b is also sent to exactly one element of Y, namely, u also. So it is true that every element of X is sent to exactly one element of Y. But f is not one-to-one because $f(a) = f(b)$ whereas $a \neq b$. *[Note that to say, "Every element of X is sent to exactly one element of Y" is just another way of saying that in the arrow diagram for the function there is only one arrow coming out of each element of X. But this statement is part of the definition of any function, not just of a one-to-one function.]*

4. *Hint:* The statement is true.

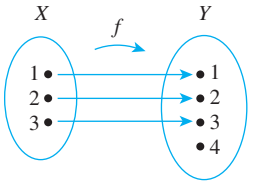
5. *Hint:* One of the incorrect ways is (b).

6. **a.** f is not one-to-one because $f(1) = 4 = f(9)$ and $1 \neq 9$. f is not onto because $f(x) \neq 3$ for any x in X.

b. g is one-to-one because $g(1) \neq g(5)$, $g(1) \neq g(9)$, and $g(5) \neq g(9)$. g is onto because each element of Y is the image of some element of X: $3 = g(5)$, $4 = g(9)$, and $7 = g(1)$.

7. **a.** F is not one-to-one because $F(c) = e = F(d)$ and $c \neq d$. F is onto because each element of Y is the image of some element of X: $e = F(c) = F(d)$, $f = F(a)$, and $g = F(b)$.

9. **a.** One example of many is the following:



10. **a.** (i) f is one-to-one. Proof: Suppose $f(n_1) = f(n_2)$ for some integers n_1 and n_2. *[We must show that $n_1 = n_2$.]* By definition of f, $2n_1 = 2n_2$, and dividing both sides by 2 gives $n_1 = n_2$ *[as was to be shown].*

(ii) f is not onto. Counterexample: Consider $1 \in \mathbf{Z}$. We claim that $1 \neq f(n)$, for any integer n, because if there were an integer n such that $1 = f(n)$, then, by definition of f, $1 = 2n$. Dividing both sides by 2 would give $n = 1/2$. But $1/2$ is not an integer. Hence $1 \neq f(n)$ for any integer n, and so f is not onto.

b. h is onto. Proof: Suppose $m \in 2\mathbf{Z}$. *[We must show that there exists an integer such that h of that integer equals m.]* Since $m \in 2\mathbf{Z}$, $m = 2k$ for some integer k. Then $h(k) = 2k = m$. Hence there exists an integer (namely, k) such that $h(k) = m$ *[as to be shown].*

11. *Hints:* **a.** (i) g is one-to-one (ii) g is not onto

b. G is onto. Proof: Suppose y is any element of $\mathbf{R}$. *[We must show that there is an element x in* $\mathbf{R}$ *such that $G(x) = y$. What would x be if it exists? Scratch work shows that x would have to equal $(y+5)/4$. The proof must then show that x has the necessary properties.]* Let $x = (y+5)/4$. Then (1) $x \in \mathbf{R}$, and (2) $G(x) = G((y+5)/4) = 4[(y+5)/4] - 5 = (y+5) - 5 = y$ *[as was to be shown].*

13. a. (i) H is not one-to-one. Counterexample: $H(1) = 1 = H(-1)$ but $1 \neq -1$.

(ii) H is not onto. Counterexample: $H(x) \neq -1$ for any real number x because $H(x) = x^2$ and no real numbers have negative squares.

14. The "proof" claims that f is one-to-one because for each integer n there is only one possible value for $f(n)$. But to say that for each integer n there is only one possible value for $f(n)$ is just another way of saying that f satisfies one of the conditions necessary for it to be a function. To show that f is one-to-one, one must show that any integer n has a *different* function value from that of the integer m whenever $n \neq m$.

15. f is one-to-one. Proof: Suppose $f(x_1) = f(x_2)$ where x_1 and x_2 are nonzero real numbers. *[We must show that* $x_1 = x_2$*.]* By definition of f,

$$\frac{x_1 + 1}{x_1} = \frac{x_2 + 1}{x_2}.$$

Cross-multiplying gives

$$x_1x_2 + x_2 = x_1x_2 + x_1,$$

and so

$$x_1 = x_2 \quad \text{by subtracting } x_1x_2 \text{ from both sides.}$$

[This is what was to be shown.]

16. f is not one-to-one. Counterexample: Note that

$$\frac{x_1}{x_1^2 + 1} = \frac{x_2}{x_2^2 + 1} \Rightarrow x_1x_2^2 + x_1 = x_2x_1^2 + x_2$$

$$\Rightarrow x_1x_2^2 - x_2x_1^2 = x_2 - x_1$$

$$\Rightarrow x_1x_2(x_2 - x_1) = x_2 - x_1$$

$$\Rightarrow x_1 = x_2 \text{ or } x_1x_2 = 1.$$

Thus for a counterexample take any x_1 and x_2 with $x_1 \neq x_2$ but $x_1x_2 = 1$. For instance, take $x_1 = 2$ and $x_2 = 1/2$. Then $f(x_1) = f(2) = 2/5$ and $f(x_2) = f(1/2) = 2/5$, but $2 \neq 1/2$.

19. a. Note that because $\frac{417302072}{7} \cong 59614581.7$ and $417302072 - 7 \cdot 59614581 = 5$, $H(417302072) = 417302072 \ mod\ 7 = 5$. But position 5 is already occupied, so the next position is checked. It is free, and thus the record is placed in position 6.

20. Recall that $\lfloor x \rfloor =$ that unique integer n such that $n \leq x < n + 1$.

a. Floor is not one-to-one. Counterexample: Floor(0) = 0 = Floor(1/2) but $0 \neq 1/2$.

b. Floor is onto. Proof: Suppose $m \in \mathbf{Z}$. *[We must show that there exists a real number y such that Floor*$(y) = m$*.]* Let $y = m$. Then Floor(y) = Floor(m) $= m$ since m is an integer. (Actually, Floor takes the value m for *all* real numbers in the interval $m \leq x < m + 1$.) Hence there exists a real number y such that Floor$(y) = m$ *[as was to be shown].*

21. a. L is not one-to-one. Counterexample: $L(0) = L(1) = 1$ but $1 \neq 0$.

b. L is onto. Proof: Suppose n is a nonnegative integer. *[We must show that there exists a string s in S such that* $L(s) = n$*.]* Let

$$s = \begin{cases} \lambda \text{(the null string)} & \text{if } n = 0 \\ \underbrace{00\ldots0}_{n\ 0\text{'s}} & \text{if } n > 0. \end{cases}$$

Then $L(s) =$ the length of $s = n$ *[as was to be shown].*

23. a. F is not one-to-one. Let $A = \{a\}$ and $B = \{b\}$. Then $F(A) = F(B) = 1$ but $A \neq B$.

24. b. N is not onto. The number -1 is in $\mathbf{Z}$ but $N(s) \neq -1$ for any string s in S because no string has a negative number of a's.

26. S is not one-to-one. Counterexample: $S(6) = 1 + 2 + 3 + 6 = 12$ and $S(11) = 1 + 11 = 12$. So $S(6) = S(11)$ but $6 \neq 11$.

S is not onto. Counterexample: In order for there to be a positive integer n such that $S(n) = 5$, n would have to be less than 5. But $S(1) = 1$, $S(2) = 3$, $S(3) = 4$, and $S(4) = 7$. Hence there is no positive integer n such that $S(n) = 5$.

27. *Hint:* **a.** T is one-to-one. **b.** T is not onto.

28. a. G is one-to-one. Proof: Suppose (x_1, y_1) and (x_2, y_2) are any elements of $\mathbf{R} \times \mathbf{R}$ such that $G(x_1, y_1) = G(x_2, y_2)$. *[We must show that* $(x_1, y_1) = (x_2, y_2)$*.]* Then, by definition of G, $(2y_1, -x_1) = (2y_2, -x_2)$, and, by definition of ordered pair,

$$2y_1 = 2y_2 \quad \text{and} \quad -x_1 = -x_2.$$

Dividing both sides of the equation on the left by 2 and both sides of the equation on the right by -1 gives that

$$y_1 = y_2 \quad \text{and} \quad x_1 = x_2,$$

and so, by definition of ordered pair, $(x_1, y_1) = (x_2, y_2)$ *[as was to be shown].*

b. G is onto. Proof: Suppose (u, v) is any element of $\mathbf{R} \times \mathbf{R}$. *[We must show that there is an element* (x, y) *in* $\mathbf{R} \times \mathbf{R}$ *such that* $G(x, y) = (u, v)$*.]* Let $(x, y) = (-v, u/2)$. Then (1) $(x, y) \in \mathbf{R} \times \mathbf{R}$ and (2) $G(x, y) = (2y, -x) = (2(u/2), -(-v)) = (u, v)$ *[as was to be shown].*

30. a. *Hint:* Use properties of rational numbers from Section 4.3 and facts about rational and irrational numbers from Sections 4.7 and 4.8.

b. *Hint:* Show that $\sqrt{3}$ is not the image of any ordered pair in $\mathbf{Q} \times \mathbf{Q}$.

31. a. *Hint: F* is one-to-one. Use the unique factorization of integers theorem in the proof.

32. a. Let $x = \log_8 27$ and $y = \log_2 3$. *[The question is: Is $x = y$?]* By definition of logarithm, both of these equations can be written in exponential form as

$$8^x = 27 \quad \text{and} \quad 2^y = 3.$$

Now $8 = 2^3$. So

$$8^x = (2^3)^x = 2^{3x}.$$

Also $27 = 3^3$ and $3 = 2^y$. So

$$27 = 3^3 = (2^y)^3 = 2^{3y}.$$

Hence, since $8^x = 27$,

$$2^{3x} = 2^{3y}.$$

By (7.2.5), then,

$$3x = 3y,$$

and so

$$x = y.$$

But $x = \log_8 27$ and $y = \log_2 3$, and so $\log_8 27 = y = \log_2 3$ and the answer to the question is yes.

33. Proof: Suppose that b, x, and y are any positive real numbers such that $b \neq 1$. Let $u = \log_b(x)$ and $v = \log_b(y)$. By definition of logarithm, $b^u = x$ and $b^v = y$. By substitution, $\frac{x}{y} = \frac{b^u}{b^v} = b^{u-v}$ *[by (7.2.3) and the fact that $b^{-v} = \frac{1}{b^v}$]*. Translating $\frac{x}{y} = b^{u-v}$ into logarithmic form gives $\log_b\left(\frac{x}{y}\right) = u - v$, and so, by substitution, $\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y)$ *[as was to be shown]*.

35. *Start of Proof:* Suppose a, b, and x are any *[particular but arbitrarily chosen]* real numbers such that b and x are positive and $b \neq 1$. *[We must show that $\log_b(x^a) = a \log_b x$.]* Let

$$r = \log_b(x^a) \text{ and } s = \log_b x.$$

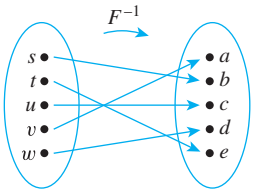
36. No. Counterexample: Define f: $\mathbf{R} \to \mathbf{R}$ and g: $\mathbf{R} \to \mathbf{R}$ as follows: $f(x) = x$ and $g(x) = -x$ for every real number x. Then f and g are both one-to-one *[because for all real numbers x_1 and x_2, if $f(x_1) = f(x_2)$ then $x_1 = x_2$, and if $g(x_1) = g(x_2)$ then $-x_1 = -x_2$, so $x_1 = x_2$ in this case as well]*. But $f + g$ is not one-to-one *[because $f + g$ satisfies the equation $(f + g)(x) = x + (-x) = 0$ for every real number x, and so, for instance, $(f + g)(1) = (f + g)(2)$ but $1 \neq 2$]*.

38. Yes. Proof: Let f be a one-to-one function from $\mathbf{R}$ to $\mathbf{R}$, and let c be any nonzero real number. Suppose $(c \cdot f)(x_1) = (c \cdot f)(x_2)$. *[We must show that $x_1 = x_2$.]* It follows by definition of $(c \cdot f)$ that $c \cdot (f(x_1)) = c \cdot (f(x_2))$. Since $c \neq 0$, we may divide both sides of the equation by c to obtain $f(x_1) = f(x_2)$. And since f is one-to-one, this implies that $x_1 = x_2$ *[as was to be shown]*.

40. a. *Hint:* The assumption that F is one-to-one is needed in the proof that $F^{-1}(F(A)) \subseteq A$. If $F(r) \in F(A)$, the definition of image of a set implies that there is an element x in A such that $F(r) = F(x)$.

b. *Hint:* The assumption that F is one-to-one is needed in the proof that $F(A_1) \cap F(A_2) \subseteq F(A_1 \cap A_2)$. If $u \in F(A_1)$ and $u \in F(A_2)$, then the definition of image of a set implies that there are elements x_1 in A_1 and x_2 in A_2 such that $F(x_1) = u$ and $F(x_2) = u$ and, thus, that $F(x_1) = F(x_2)$.

42.



44. The function is not a one-to-one correspondence because it is not onto.

45. The answer to exercise 10(b) shows that h is onto. To show that h is one-to-one, suppose $h(n_1) = h(n_2)$. By definition of h, this implies that $2n_1 = 2n_2$. Dividing both sides by 2 gives $n_1 = n_2$. Hence h is one-to-one, and so h is a one-to-one correspondence.

Given any even integer m, if $m = h(n)$, then by definition of h, $m = 2n$, and so $n = m/2$. Thus

$$h^{-1}(m) = \frac{m}{2} \text{ for every } m \in 2\mathbf{Z}.$$

46. The function g is not a one-to-one correspondence because it is not onto. For instance, if $m = 2$, it is impossible to find an integer n such that $g(n) = m$. (This is because if $g(n) = m$, then $4n - 5 = 2$, which implies that $n = 7/4$. Thus the only number n with the property that $g(n) = m$ is $7/4$. But $7/4$ is not an integer.)

47. The answer to exercise 11b shows that G is onto. In addition, G is one-to-one. To prove this, suppose $G(x_1) = G(x_2)$ for some x_1 and x_2 in $\mathbf{R}$. *[We must show that $x_1 = x_2$.]* By definition of G, $4x_1 - 5 = 4x_2 - 5$. Add 5 to both sides of this equation and divide both sides by 4 to obtain $x_1 = x_2$ *[as was to be shown]*. We claim that $G^{-1}(y) = (y + 5)/4$ for each y in $\mathbf{R}$. By definition of inverse function, this is true if, and only if, $G((y + 5)/4) = y$. But

$G((y+5)/4) = 4((y+5)/4) - 5 = (y+5) - 5 = y$, and so it is the case that $G^{-1}(y) = (y+5)/4$ for each y in $\mathbf{R}$.

50. The function L is not a one-to-one correspondence because it is not one-to-one.

52. The answer to exercise 15 shows that f is one-to-one, and if the co-domain is taken to be the set of all real numbers not equal to 1, then f is also onto. The reason is that given any real number $y \neq 1$, if we take $x = \frac{1}{y-1}$, then x is a real number and

$$f(x) = f\left(\frac{1}{y-1}\right) = \frac{\frac{1}{y-1}+1}{\frac{1}{y-1}} = \frac{1+(y-1)}{1} = y.$$

Thus $f^{-1}(y) = \frac{1}{y-1}$ for each real number $y \neq 1$.

53. The answer to exercise 16 in Appendix B shows that f is not one-to-one. Therefore, it is not a one-to-one correspondence.

57. *Hint:* Let a function F be given and suppose the domain of F is represented as a one-dimensional array $a[1], a[2], \ldots, a[n]$. Introduce a variable *answer* whose initial value is "one-to-one." The main part of the body of the algorithm could be written as follows:

while ($i \leq n-1$ and *answer* = "one-to-one")
  $j := i+1$
  while ($j \leq n$ and *answer* = "one-to-one")
    if ($F(a[i]) = F(a[j])$ and $a[i] \neq a[j]$)
    then *answer* := "not one-to-one"
    $j := j+1$
  end while
  $i := i+1$
end while

What can you say if execution reaches this point?

58. *Hint:* Let a function F be given and suppose the domain and co-domain of F are represented by the one-dimensional arrays $a[1], a[2], \ldots, a[n]$ and $b[1], b[2], \ldots, b[m]$, respectively. Introduce a variable *answer* whose initial value is "onto." For each $b[i]$ from $i = 1$ to m, make a search through $a[1], a[2], \ldots, a[n]$ to check whether $b[i] = F(a[j])$ for some $a[j]$. Introduce a Boolean variable to indicate whether a search has been successful. (Set the variable equal to 0 before the start of each search, and let it have the value 1 if the search is successful.) At the end of each search, check the value of the Boolean variable. If it is 0, then F is not onto. If all searches are successful, then F is onto.

SECTION 7.3

1. $g \circ f$ is defined as follows:

$$(g \circ f)(1) = g(f(1)) = g(5) = 1$$
$$(g \circ f)(3) = g(f(3)) = g(3) = 5$$
$$(g \circ f)(5) = g(f(5)) = g(1) = 3.$$

$f \circ g$ is defined as follows:

$$(f \circ g)(1) = f(g(1)) = f(3) = 3$$
$$(f \circ g)(3) = f(g(3)) = f(5) = 1$$
$$(f \circ g)(5) = f(g(5)) = f(1) = 5.$$

Then $g \circ f \neq f \circ g$ because, for example, $(g \circ f)(1) \neq (f \circ g)(1)$.

3. $(G \circ F)(x) = G(F(x)) = G(x^3) = x^3 - 1$ for every real number x.

$(F \circ G)(x) = F(G(x)) = F(x-1) = (x-1)^3$ for every real number x.

$G \circ F \neq F \circ G$ because, for instance, $(G \circ F)(2) = 2^3 - 1 = 7$, whereas $(F \circ G)(2) = (2-1)^3 = 1$.

6. $(G \circ F)(0) = G(F(0)) = G(7 \cdot 0) = G(0)$
$= 0 \ mod \ 5 = 0$

$(G \circ F)(1) = G(F(1)) = G(7 \cdot 1) = G(7)$
$= 7 \ mod \ 5 = 2$

$(G \circ F)(2) = G(F(2)) = G(7 \cdot 2) = G(14)$
$= 14 \ mod \ 5 = 4$

$(G \circ F)(3) = G(F(3)) = G(7 \cdot 3) = G(21)$
$= 21 \ mod \ 5 = 1$

$(G \circ F)(4) = G(F(4)) = G(7 \cdot 4) = G(28)$
$= 28 \ mod \ 5 = 3$

7. a. *Partial answer:*

$(L \circ M)(12) = L(M(12)) = L(12 \ mod \ 5) = L(2)$
$= 2^2 = 4$

$(M \circ L)(12) = M(L(12)) = M(12^2) = M(144)$
$= 144 \ mod \ 5 = 4$

8. a. $(T \circ L)(abaa) = T(L(abaa)) = T(4)$
$= 4 \ mod \ 3 = 1$

9. a. $(G \circ F)(2) = G(F(2)) = G(2^2/3) = G(4/3) = \lfloor 4/3 \rfloor = 1$

10. a. $(G \circ F)(8) = G(F(8)) = G(16) = \lfloor 16/2 \rfloor = 8$
$(F \circ G)(8) = F(G(8)) = F(\lfloor 8/2 \rfloor) = F(4) = 8$
$(G \circ F)(3) = G(F(3)) = G(6) = \lfloor 6/2 \rfloor = 3$
$(F \circ G)(3) = F(G(3)) = F(\lfloor 3/2 \rfloor) = F(1) = 2$

b. $G \circ F \neq F \circ G$ because $(G \circ F)(3) = (F \circ G)(3) = 2$ and $3 \neq 2$.

12. $(F^{-1} \circ F)(x) = F^{-1}(F(x)) = F^{-1}(3x+2)$
$= \frac{(3x+2)-2}{3} = \frac{3x}{3} = x = I_{\mathbf{R}}(x)$

for every x in $\mathbf{R}$. Hence $F^{-1} \circ F = I_{\mathbf{R}}$ by definition of equality of functions.

$$(F \circ F^{-1})(y) = F(F^{-1}(y)) = F\left(\frac{y-2}{3}\right)$$
$$= 3\left(\frac{y-2}{3}\right) + 2 = (y-2) + 2$$
$$= y = I_{\mathbf{R}}(y)$$

for every y in $\mathbf{R}$. Hence $F \circ F^{-1} = I_{\mathbf{R}}$ by definition of equality of functions.

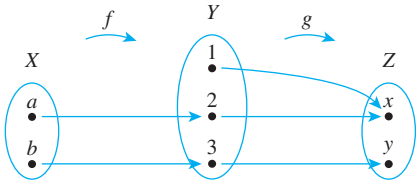
15. a. By definition of logarithm with base b, for each real number x, $\log_b(b^x)$ is the exponent to which b must be raised to obtain b^x. But this exponent is just x. So $\log_b(b^x) = x$.

16. *Hint:* Suppose f is any function from a set X to a set Y, and show that for every x in X, $(I_Y \circ f)(x) = f(x)$.

18. a. $s_k = s_m$

19. The answer is no.

Counterexample: Define f and g by the arrow diagrams below.



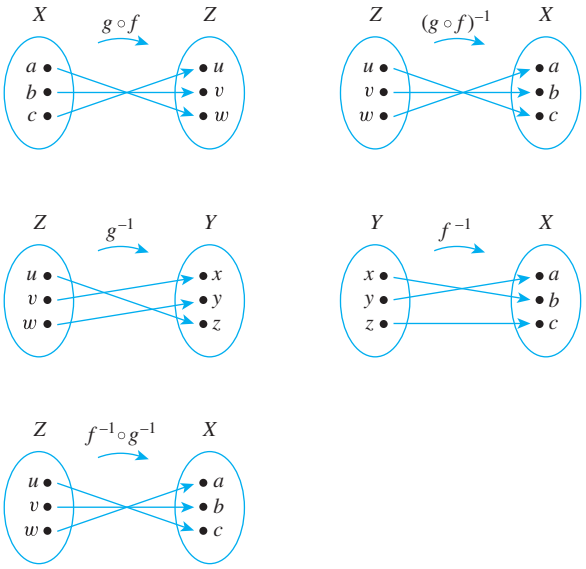
Then $g \circ f$ is one-to-one but g is not one-to-one. (This is one counterexample among many. Can you construct a different one?)

21. *Hint:* Suppose $f: X \to Y$ and $g: Y \to Z$ are functions and $g \circ f$ is one-to-one. Given x_1 and x_2 in X, if $f(x_1) = f(x_2)$ then $(g \circ f)(x_1) = (g \circ f)(x_2)$. (Why?) Then use the fact that $g \circ f$ is one-to-one.

22. *Hint:* Suppose $f: X \to Y$ and $g: Y \to Z$ are functions and $g \circ f$ is onto. Given $z \in Z$, there is an element x in X such that $(g \circ f)(x) = z$. (Why?) If $y = f(x)$, what can you deduce about $g(y)$?

24. True. Proof: Suppose X is any set and f, g, and h are functions from X to X such that h is one-to-one and $h \circ f = h \circ g$. *[We must show that for every x in X, $f(x) = g(x)$.]* Suppose x is any element in X. Because $h \circ f = h \circ g$, we have that $(h \circ f)(x) = (h \circ g)(x)$ by definition of equality of functions. Then, by definition of composition of functions, $h(f(x)) = h(g(x))$. And since h is one-to-one, this implies that $f(x) = g(x)$ *[as was to be shown]*.

26.



The functions $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ are equal.

29. *Hints:* (1) Theorems 7.3.3 and 7.3.4 taken together insure that $g \circ f$ is one-to-one and onto. (2) Use the inverse function property: $F^{-1}(b) = a \Leftrightarrow F(a) = b$, for every a in the domain of F and every b in the domain of F^{-1}.

SECTION 7.4

1. The student should have replied that for A to have the same cardinality as B means that there is a function from A to B that is one-to-one and onto. A set cannot have the property of being onto or one-to-one another set; only a function can have these properties.

2. Define a function $f: \mathbf{Z}^+ \to S$ as follows: For every positive integer k, $f(k) = k^2$.

f is one-to-one: [We must show that for all k_1 and $k_2 \in \mathbf{Z}^+$, if $f(k_1) = f(k_2)$ then $k_1 = k_2$.] Suppose k_1 and k_2 are positive integers and $f(k_1) = f(k_2)$. By definition of f, $(k_1)^2 = (k_2)^2$, so $k_1 = \pm k_2$. But k_1 and k_2 are *positive*. Hence $k_1 = k_2$.

f is onto: [We must show that for each $n \in S$, there exists $k \in \mathbf{Z}^+$ such that $n = f(k)$.] Suppose $n \in S$. By definition of S, $n = k^2$ for some positive integer k. Then by definition of f, $n = f(k)$.

Since there is a one-to-one, onto function (namely, f) from $\mathbf{Z}^+$ to S, the two sets have the same cardinality.

3. Define $f: \mathbf{Z} \to 3\mathbf{Z}$ by the rule $f(n) = 3n$ for each integer n.

The function f is one-to-one because for any integers n_1 and n_2, if $f(n_1) = f(n_2)$ then $3n_1 = 3n_2$ and so $n_1 = n_2$.

Also f is onto because if m is any element in $3\mathbf{Z}$, then $m = 3k$ for some integer k. Then $f(k) = 3k = m$ by definition of f. Thus, since there is a function $f\colon \mathbf{Z} \to 3\mathbf{Z}$ that is one-to-one and onto, $\mathbf{Z}$ has the same cardinality as $3\mathbf{Z}$.

6. *Hint:* If $m \in 2\mathbf{Z}$, show that $J(m) = J(m+1) = m$.

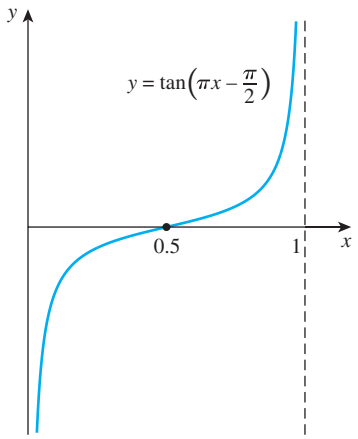
7. b. For each positive integer n, $F(n) = (-1)^n \left\lfloor \frac{n}{2} \right\rfloor$.

8. It was shown in Example 7.4.2 that $\mathbf{Z}$ is countably infinite, which means that $\mathbf{Z}^+$ has the same cardinality as $\mathbf{Z}$. By exercise 3, $\mathbf{Z}$ has the same cardinality as $3\mathbf{Z}$. It follows by the transitive property of cardinality (Theorem 7.4.1 (c)) that $\mathbf{Z}^+$ has the same cardinality as $3\mathbf{Z}$. Thus $3\mathbf{Z}$ is countably infinite *[by definition of countably infinite]*, and hence $3\mathbf{Z}$ is countable *[by definition of countable]*.

10. Proof: Define $f\colon S \to U$ by the rule $f(x) = 2x$ for each real number x in S. Then f is one-to-one by the same argument as in exercise 10a of Section 7.2 with $\mathbf{R}$ in place of $\mathbf{Z}$. Furthermore, f is onto because if y is any element in U, then $0 < y < 2$ and so $0 < y/2 < 1$. Consequently, $y/2 \in S$ and $f(y/2) = 2(y/2) = y$. Hence f is a one-to-one correspondence, and so S and U have the same cardinality.

11. *Hint:* Define $h\colon S \to V$ as follows: $h(x) = 3x + 2$, for every $x \in S$.

13.



It is clear from the graph that f is one-to-one (since it is increasing) and that the image of f is all of $\mathbf{R}$ (since the lines $x = 0$ and $x = 1$ are vertical asymptotes). Thus S and $\mathbf{R}$ have the same cardinality.

16. In Example 7.4.4 it was shown that there is a one-to-one correspondence from $\mathbf{Z}^+$ to $\mathbf{Q}^+$. This implies that the positive rational numbers can be written as an infinite sequence: $r_1, r_2, r_3, r_4, \ldots$. Now the set $\mathbf{Q}$ of all rational numbers consists of the numbers in this sequence together with 0 and the negative rational numbers:

$$-r_1, -r_2, -r_3, -r_4, \ldots.$$

Let $r_0 = 0$. Then the elements of the set of all rational numbers can be "counted" as follows:

$$r_0, r_1, -r_1, r_2, -r_2, r_3, -r_3, r_4, -r_4, \ldots.$$

In other words, we can define a one-to-one correspondence as follows: for each integer $n \geq 1$,

$$G(n) = \begin{cases} r_{n/2} & \text{if } n \text{ is even} \\ -r_{(n-1)/2} & \text{if } n \text{ is odd} \end{cases}$$

Therefore, $\mathbf{Q}$ is countably infinite and hence countable.

17. *Hint:* See the hints for exercises 18 and 19 in Section 4.3.

18. *Hint:* No.

19. *Hint:* Suppose r and s are real numbers with $s > r > 0$. Let n be an integer such that $n > \frac{\sqrt{2}}{s-r}$, and let $m = \left\lfloor \frac{nr}{\sqrt{2}} \right\rfloor + 1$. Show that $m > \frac{nr}{\sqrt{2}} \geq m - 1$, and use the fact that $s = r + (s - r)$ to conclude that $r < \frac{\sqrt{2}m}{n} < s$.

22. *Hint:* Use the unique factorization of integers theorem (Theorem 4.4.5) and Theorem 7.4.3.

23. a. Define a function $G\colon \mathbf{Z}^{nonneg} \to \mathbf{Z}^{nonneg} \times \mathbf{Z}^{nonneg}$ as follows: Let $G(0) = (0, 0)$, and then follow the arrows in the diagram, letting each successive ordered pair of integers be the value of G for the next successive integer. Thus, for instance, $G(1) = (1, 0)$, $G(2) = (0, 1)$, $G(3) = (2, 0)$, $G(4) = (1, 1)$, $G(5) = (0, 2)$, $G(6) = (3, 0)$, $G(7) = (2, 1)$, $G(8) = (1, 2)$, and so forth.

b. *Hint:* Observe that if the top ordered pair of any given diagonal is $(k, 0)$, the entire diagonal (moving from top to bottom) consists of $(k, 0)$, $(k-1, 1)$, $(k-2, 2), \ldots,$ $(2, k-2)$, $(1, k-1)$, $(0, k)$. Thus for every ordered pair (m, n) within any given diagonal, the value of $m + n$ is constant, and as you move down the ordered pairs in the diagonal, starting at the top, the value of the second element of the pair keeps increasing by 1.

25. *Hint:* There are at least two different approaches to this problem. One is to use the method discussed in Section 4.3. Another is to suppose that $1.999999\ldots < 2$ and derive a contradiction. (Show that the difference between 2 and $1.999999\ldots$ can be made smaller than any given positive number.)

26. Proof: Let A be an infinite set. Construct a countably infinite subset $a_1, a_2, a_3, \ldots$ of A, by letting a_1 be any element of A, letting a_2 be any element of A other than a_1, letting a_3 be any element of A other than a_1 or a_2, and so forth. This process never stops (and hence $a_1, a_2, a_3, \ldots$ is an infinite sequence) because A is an infinite set. More formally,

1. Let a_1 be any element of A.
2. For each integer $n \neq 2$, let a_n be any element of $A - \{a_1, a_2, a_3, \ldots, a_{n-1}\}$. Such an element exists, for otherwise $A - \{a_1, a_2, a_3, \ldots, a_{n-1}\}$ would be empty and A would be finite.

27. Proof: Suppose A is any countably infinite set, B is any set, and $g: A \to B$ is onto. Since A is countably infinite, there is a one-to-one correspondence $f: \mathbf{Z}^+ \to A$. Then, in particular, f is onto, and so by Theorem 7.3.4, $g \circ f$ is an onto function from $\mathbf{Z}^+$ to B. Define a function h: $B \to \mathbf{Z}^+$ as follows: Suppose x is any element of B. Since $g \circ f$ is onto, $\{m \in \mathbf{Z}^+ \mid (g \circ f)(m) = x\} \neq \emptyset$. Thus, by the well-ordering principle for the integers, this set has a least element. In other words, there is a least positive integer n with $(g \circ f)(n) = x$. Let $h(x)$ be this integer.

We claim that h is a one-to-one. Suppose $h(x_1) = h(x_2) = n$. By definition of h, n is the least positive integer with $(g \circ f)(n) = x_1$. Moreover, by definition of h, n is the least positive integer with $(g \circ f)(n) = x_2$. Hence $x_1 = (g \circ f)(n) = x_2$.

Thus h is a one-to-one correspondence between B and a subset S of positive integers (the range of h). Since any subset of a countable set is countable (Theorem 7.4.3), S is countable, and so there is a one-to-one correspondence between B and a countable set. It follows from the transitive property of cardinality that B is countable.

29. *Hint:* Suppose A and B are any two countably infinite sets. Then there are one-to-one correspondences $f: \mathbf{Z}^+ \to A$ and $g: \mathbf{Z}^+ \to B$.

Case 1 ($A \cap B = \emptyset$): In this case define $h: \mathbf{Z}^+ \to A \cup B$ as follows: For every integer $n \geq 1$,

$$h(n) = \begin{cases} f(n/2) & \text{if } n \text{ is even} \\ g((n+1)/2) & \text{if } n \text{ is odd.} \end{cases}$$

Show that h is one-to-one and onto.

Case 2 ($A \cap B \notin \emptyset$): In this case let $C = B - A$. Then $A \cup B = A \cup C$ and $A \cap C = \emptyset$. If C is countably infinite, use the result of case 1 to complete the proof. If C is finite, use the result of exercise 28 to complete the proof.

30. *Hint:* Use proof by contradiction and the fact that the set of all real numbers is uncountable.

31. *Hint:* Consider the following cases: (1) A and B are both finite, (2) at least one of A or B is infinite and $A \cap B = \emptyset$, (3) at least one of A or B is infinite and $A \cap B \neq \emptyset$. In case 3 use the fact that $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ and that the sets $(A - B)$, $(B - A)$, and $(A \cap B)$ are mutually disjoint.

32. *Hint:* Use the one-to-one correspondence $F: \mathbf{Z}^+ \to \mathbf{Z}$ of Example 7.4.2 to define a function $G: \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z} \times \mathbf{Z}$ by the formula $G(m, n) = (F(m), F(n))$. Show that G is a one-to-one correspondence, and use the result of exercise 22 and the transitive property of cardinality.

34. *Hint for Solution 1:* Define a function $f: \mathcal{P}(S) \to T$ as follows: For each subset A of S, let $f(A) = \chi_A$, the *characteristic function* of A, where $\chi_A: S \to \{0, 1\}$ is defined by the rule

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \text{ for every } x \in S. \end{cases}$$

Show that f is one-to-one (for all subsets A_1 and A_2 in S, if $\chi_{A_1} = \chi_{A_2}$ then $A_1 = A_2$) and that f is onto (given any function $g: S \to \{0, 1\}$, there is a subset A of S such that $g = \chi_A$).

Hint for Solution 2: Define $H: T \to \mathcal{P}(S)$ by letting $H(f) = \{x \in S \mid f(x) = 1\}$. Show that H is a one-to-one correspondence.

35. Partial proof (by contradiction): Suppose not. Suppose there is a one-to-one, onto function $f: S \to \mathcal{P}(S)$. Let

$$A = \{x \in S \mid x \notin f(x)\}.$$

Then $A \in \mathcal{P}(S)$ and since f is onto, there exists $z \in S$ such that $A = f(z)$. *[Now derive a contradiction!]*

37. *Hint:* Since A and B are countable, their elements can be listed as

$$A: a_1, a_2, a_3, \ldots \quad \text{and} \quad B: b_1, b_2, b_3, \ldots$$

Represent the elements of $A \times B$ in a grid:

$$\begin{array}{lll} (a_1, b_1) & (a_1, b_2) & (a_1, b_3) \ \ldots \\ (a_2, b_1) & (a_2, b_2) & (a_2, b_3) \ \ldots \\ (a_3, b_1) & (a_3, b_2) & (a_3, b_3) \ \ldots \\ \vdots & \vdots & \vdots \end{array}$$

Now use a counting method similar to that of Example 7.4.4.

SECTION 8.1

1. a. $0 \, E \, 0$ because $0 - 0 = 0 = 2 \cdot 0$, so $2 \mid (0 - 0)$.
$5 \not E \, 2$ because $5 - 2 = 3$ and $3 \neq 2k$ for any integer k, so $2 \nmid (5 - 2)$.
$(6, 6) \in E$ because $6 - 6 = 0 = 2 \cdot 0$, so $2 \mid (6 - 6)$.
$(-1, 7) \in E$ because $-1 - 7 = -8 = 2 \cdot (-4)$, so $2 \mid (-1 - 7)$.

2. *Hint:* To prove a statement of the form $p \leftrightarrow (q \vee r)$, you need to prove both (1) $p \to (q \vee r)$ and (2) $(q \vee r) \to p$. The easiest way to prove $p \to (q \vee r)$ is to prove the logically equivalent statement form $(p \wedge \sim q) \to r$. And the easiest way to prove $(q \vee r) \to p$ is to prove the

logically equivalent statement form $(q \rightarrow p) \wedge (r \rightarrow p)$. In this case, suppose m and n are any integers, and let p be "$m - n$ is even," let q be "both m and n are even," and let r be "both m and n are odd."

3. a. $10\ T\ 1$ because $10 - 1 = 9 = 3 \cdot 3$, and so $3 \mid (10 - 1)$.
$1\ T\ 10$ because $1 - 10 = -9 = 3 \cdot (-3)$, and so $3 \mid (1 - 10)$.
$2\ T\ 2$ because $2 - 2 = 0 = 3 \cdot 0$, and so $3 \mid (2 - 2)$.
$8\ \not{T}\ 1$ because $8 - 1 = 7 \neq 3k$, for any integer k. So $3 \nmid (8 - 1)$.

b. *One possible answer:* 3, 6, 9, −3, −6

e. *Hint:* All integers of the form $3k + 1$, for some integer k, are related by T to 1.

4. a. Yes, because 15 and 25 are both divisible by 5, which is prime.

b. No, because 22 and 27 have no common prime factor.

5. a. Yes, because both $\{a, b\}$ and $\{b, c\}$ have two elements.

6. a. No, because $\{a\} \cap \{c\} = \varnothing$.

7. a. Yes. $1\ R\ (-9) \Leftrightarrow 5 \mid (1^2 - (-9)^2)$. But $1^2 - (-9)^2 = 1 - 81 = -80$, and $5 \mid (-80)$ because $-80 = 5 \cdot (-16)$.

8. a. Yes, because both *abaa* and *abba* have the same first two characters *ab*.

b. No, because the first two characters of *aabb* are different from the first two characters of *bbaa*.

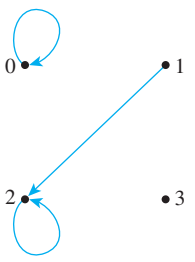
9. a. Yes, because the sum of the characters in 0121 is 4 and the sum of the characters in 2200 is also 4.

b. No, because the sum of the characters in 1011 is 3, whereas the sum of the characters in 2101 is 4.

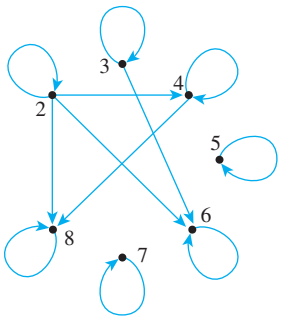
10. $R = \{(3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\}$
$R^{-1} = \{(4, 3), (5, 3), (6, 3), (5, 4), (6, 4), (6, 5)\}$

12. a. No. If $F: X \rightarrow Y$ is not onto, then F^{-1} fails to be defined on all of Y. In other words, there is an element y in Y such that $(y, x) \notin F^{-1}$ for any $x \in X$. Consequently, F^{-1} does not satisfy property (1) of the definition of function.

13.



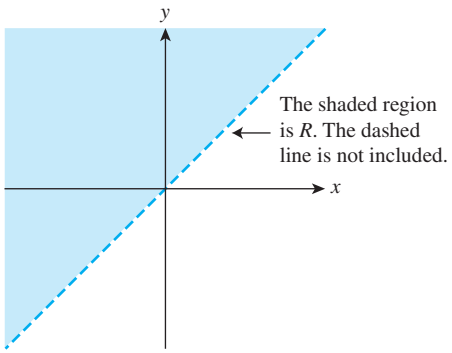
15.

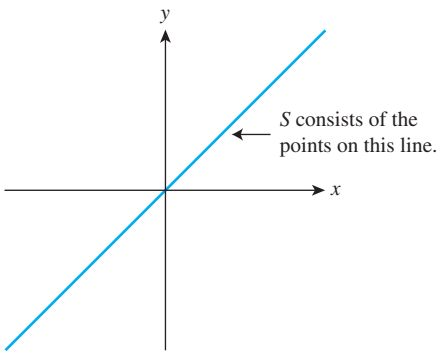


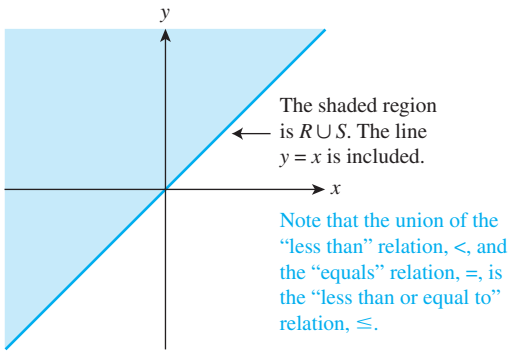
16. *Hint:* See Example 8.1.6.

19. $A \times B = \{(2, 6), (2, 8), (2, 10), (4, 6), (4, 8), (4, 10)\}$
$R = \{(2, 6), (2, 8), (2, 10), (4, 8)\}$
$S = \{(2, 6), (4, 8)\}$
$R \cup S = R,\ R \cap S = S$

21.







Note that the union of the "less than" relation, $<$, and the "equals" relation, $=$, is the "less than or equal to" relation, $\leq$.

The graph of the intersection of R and S is obtained by finding the set of all points common to both graphs. But there are no points for which both $x < y$ and $x = y$. Hence $R \cap S = \varnothing$ and the graph consists of no points at all.

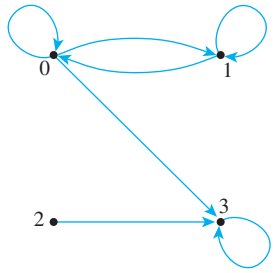
24. a.

574329	Tak Kurosawa
011985	John Schmidt

SECTION 8.2

1. R_1:

a.



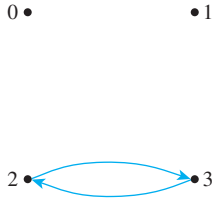
b. R_1 is not reflexive: $2 \not R_1 2$.

c. R_1 is not symmetric: $2\ R_1\ 3$ but $3 \not R_1\ 2$.

d. R_1 is not transitive: $1\ R_1\ 0$ and $0\ R_1\ 3$ but $1 \not R_1\ 3$.

3. R_3:

a.



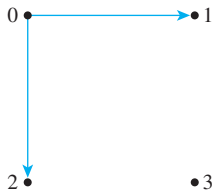
b. R_3 is not reflexive: $(0, 0) \notin R_3$.

c. R_3 is symmetric. (If R_3 were not symmetric, there would be elements x and y in $A = \{0, 1, 2, 3\}$ such that $(x, y) \in R_3$ but $(y, x) \notin R_3$. It is clear by inspection that no such elements exist.)

d. R_3 is not transitive: $(2, 3) \in R_3$ and $(3, 2) \in R_3$ but $(2, 2) \notin R_3$.

6. R_6:

a.



b. R_6 is not reflexive: $(0, 0) \notin R_6$.

c. R_6 is not symmetric: $(0, 1) \in R_6$ but $(1, 0) \notin R_6$.

d. R_6 is transitive. (If R_6 were not transitive, there would be elements x, y, and z in $\{0, 1, 2, 3\}$ such that $(x, y) \in R_6$ and $(y, z) \in R_6$ and $(x, z) \notin R_6$. It is clear by inspection that no such elements exist.)

9. ***R is reflexive:*** R is reflexive $\Leftrightarrow$ for every real number x, $x\ R\ x$. By definition of R, this means that for every real number x, $x \geq x$. In other words, for every real number x, $x > x$ or $x = x$, which is true.

R is not symmetric: R is symmetric $\Leftrightarrow$ for all real numbers x and y, if $x\ R\ y$ then $y\ R\ x$. By definition of R, this means that for all real numbers x and y, if $x \geq y$ then $y \geq x$. The following counterexample shows that this is false. $x = 1$ and $y = 0$. Then $x \geq y$, but $y \not\geq x$ because $1 \geq 0$ and $0 \not\geq 1$.

R is transitive: R is transitive $\Leftrightarrow$ for all real numbers x, y, and z, if $x\ R\ y$ and $y\ R\ z$ then $x\ R\ z$. By definition of R, this means that for all real numbers x, y, and z, if $x \geq y$ and $y \geq z$ then $x \geq z$. This is true by definition of $\geq$ and the transitive property of order for the real numbers. (See Appendix A, T18.)

11. ***D is reflexive:*** For D to be reflexive means that for every real number x, $x\ D\ x$. By definition of D, this means that for every real number x, $xx = x^2 \geq 0$, which is true.

D is symmetric: For D to be symmetric means that for all real numbers x and y, if $x\ D\ y$ then $y\ D\ x$. By definition of D, this means that for all real numbers x and y, if $xy \geq 0$ then $yx \geq 0$, which is true by the commutative law of multiplication.

D is not transitive: For D to be transitive means that for all real numbers x, y, and z, if $x\ D\ y$ and $y\ D\ z$ then $x\ D\ z$. By definition of D, this means that for all real numbers x, y, and z, if $xy \geq 0$ and $yz \geq 0$ then $xz \geq 0$. This is false because there exist real numbers x, y, and z such that $xy \geq 0$ and $yz \geq 0$ but $xz \not\geq 0$. As a counterexample, let $x = 1$, $y = 0$, and $z = -1$. Then $x\ D\ y$ and $y\ D\ z$ because $1 \cdot 0 \geq 0$ and $0 \cdot (-1) \geq 0$. But $x \not D\ z$ because $1 \cdot (-1) \not\geq 0$.

12. ***E is reflexive:*** *[We must show that for every integer m, m E m.]* Suppose m is any integer. Since $m - m = 0$ and $4 \mid 0$, we have that $4 \mid (m - m)$. Consequently, $m\ E\ m$ by definition of E.

E is symmetric: *[We must show that for all integers m and n, if m E n then n E m.]* Suppose m and n are any integers such that $m\ E\ n$. By definition of E, this means that $4 \mid (m - n)$, and so, by definition of divisibility, $m - n = 4r$ for some integer r. Now $n - m = -(m - n)$. Hence, by substitution, $n - m = -(4r) = 4(-r)$. It follows that $4 \mid (n - m)$ by definition of divisibility (since $-r$ is an integer), and thus $n\ E\ m$ by definition of E.

E is transitive: *[We must show that for all integers m, n, and p if m E n and n E p then m E p.]* Suppose m, n, and p are any integers such that $m\ E\ n$ and $n\ E\ p$. By definition of E this means that $4 \mid (m - n)$ and $4 \mid (n - p)$, and so, by definition of divisibility, $m - n = 4r$ for some integer r and $n - p = 4s$ for some integer s. Now $m - p = (m - n) + (n - p)$. Hence, by substitution, $m - p = 4r + 4s = 4(r + s)$. It follows that $4 \mid (m - p)$ by definition of divisibility (since $r + s$ is an integer), and thus $m\ E\ p$ by definition of E.

15. ***D is reflexive:*** *[We must show that for every positive integer m, m D m.]* Suppose m is any positive integer. Since $m = m \cdot 1$, by definition of divisibility $m \mid m$. Hence $m\ D\ m$ by definition of D.

D is not symmetric: For D to be symmetric would mean that for all positive integers m and n, if $m\ D\ n$ then $n\ D\ m$. By definition of divisibility, this would mean that for all positive integers m and n, if $m \mid n$ then $n \mid m$. A counterexample shows that this is false. Let $m = 2$ and $n = 4$. Then $m \mid n$ because $2 \mid 4$ but $n \nmid m$ because $4 \nmid 2$.

D is transitive: To prove transitivity of D, we must show that for all positive integers m, n, and p, if $m\ D\ n$ and $n\ D\ p$ then $m\ D\ p$. By definition of D, this means that for all positive integers m, n, and p, if $m \mid n$ and $n \mid p$ then $m \mid p$. But this is true by Theorem 4.4.3 (the transitivity of divisibility).

18. *Hint:* Q is reflexive, symmetric, and transitive.

20. ***E is reflexive:*** $\mathbf{E}$ is reflexive $\Leftrightarrow$ for every subset A of X, $A\ \mathbf{E}\ A$. By definition of $\mathbf{E}$, this means that for every subset A of X, A has the same number of elements as A, which is true.

E is symmetric: $\mathbf{E}$ is symmetric $\Leftrightarrow$ for all subsets A and B of X, if $A\ \mathbf{E}\ B$ then $B\ \mathbf{E}\ A$. By definition of $\mathbf{E}$, this means that if A has the same number of elements as B, then B has the same number of elements as A, which is true.

E is transitive: $\mathbf{E}$ is transitive $\Leftrightarrow$ for all subsets A, B, and C of X, if $A\ \mathbf{E}\ B$ and $B\ \mathbf{E}\ C$ then $A\ \mathbf{E}\ C$. By definition of $\mathbf{E}$, this means that for all subsets, A, B, and C of X, if A has the same number of elements as B and B has the number of elements as C, then A has the same number of elements as C, which is true.

23. ***S is reflexive:*** $\mathbf{S}$ is reflexive $\Leftrightarrow$ for every subset A of X, $A\ \mathbf{S}\ A$. By definition of $\mathbf{S}$, this means that for every subset A of X, $A \subseteq A$. This is true because every set is a subset of itself.

S is not symmetric: $\mathbf{S}$ is symmetric $\Leftrightarrow$ for all subsets A and B of X, if $A\ \mathbf{S}\ B$ then $B\ \mathbf{S}\ A$. By definition of $\mathbf{S}$, this means that for all subsets A and B of X, if $A \subseteq B$ then $B \subseteq A$. This is false because $X \neq \varnothing$ and so there is an element, say a, in X. As a counterexample, take $A = \varnothing$ and $B = \{a\}$. Then $A \subseteq B$ but $B \not\subseteq A$.

S is transitive: $\mathbf{S}$ is transitive $\Leftrightarrow$ for all subsets A, B, and C of X, if $A\ \mathbf{S}\ B$ and $B\ \mathbf{S}\ C$, then $A\ \mathbf{S}\ C$. By definition of $\mathbf{S}$, this means that for all subsets A, B, and C of X, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$, which is true by the transitive property of subsets (Theorem 6.2.1 (3)).

25. ***R is reflexive:*** Suppose s is any string in A. Then $s\ R\ s$ because s has the same first two characters as s.

R is symmetric: Suppose s and t are any strings in A such that $s\ R\ t$. By definition of R, s has the same first two characters as t. It follows that t has the same first two characters as s, and so $t\ R\ s$.

R is transitive: Suppose s, t, and u are any strings in A such that $s\ R\ t$ and $t\ R\ u$. By definition of R, s has the same first two characters as t and t has the same first two characters as u. It follows that s has the same two characters as u, and so $s\ R\ u$.

27. ***I is reflexive:*** *[We must show that for every statement p, p* $\mathbf{I}$ *p.]* Suppose p is a statement. The only way a conditional statement can be false is for its hypothesis to be true and its conclusion false. Consider the statement $p \rightarrow p$. Both the hypothesis and the conclusion have the same truth value. Thus it is impossible for $p \rightarrow p$ to be false, and so $p \rightarrow p$ must be true.

I is not symmetric: $\mathbf{I}$ is symmetric $\Leftrightarrow$ for all statements p and q, if $p\ \mathbf{I}\ q$ then $q\ \mathbf{I}\ p$. By definition of $\mathbf{I}$, this means that for all statements p and q, if $p \rightarrow q$ then $q \rightarrow p$. But this is false: there are statements p and q such that $p \rightarrow q$ is true and $q \rightarrow p$ is false. For instance, let p be "10 is divisible by 4" and let q be "10 is divisible by 2." Then $p \rightarrow q$ is "If 10 is divisible by 4, then 10 is divisible by 2." This is true because its hypothesis, p, is false. On the other hand, $q \rightarrow p$ is "If 10 is divisible by 2, then 10 is divisible by 4." This is false because its hypothesis, q, is true and its conclusion, p, is false.

I is transitive: *[We must show that for all statements p, q, and r, if p* $\mathbf{I}$ *q and q* $\mathbf{I}$ *r then p* $\mathbf{I}$ *r.]* Suppose p, q, and r are statements such that $p\ \mathbf{I}\ q$ and $q\ \mathbf{I}\ r$. By definition of $\mathbf{I}$, this means that $p \rightarrow q$ and $q \rightarrow r$ are both true. By transitivity of if-then (Example 2.3.6 and exercise 20 of Section 2.3), we can conclude that $p \rightarrow r$ is true. Hence, by definition of $\mathbf{I}$, $p\ \mathbf{I}\ r$.

28. ***F is reflexive:*** $\mathbf{F}$ is reflexive $\Leftrightarrow$ for all elements (x, y) in $\mathbf{R} \times \mathbf{R}$, $(x, y)\ \mathbf{F}\ (x, y)$. By definition of $\mathbf{F}$, this means that for all elements (x, y) in $\mathbf{R} \times \mathbf{R}$, $x = x$, which is true.

F is symmetric: *[We must show that for all elements* (x_1, y_1) *and* (x_2, y_2) *in* $\mathbf{R} \times \mathbf{R}$, *if* $(x_1, y_1)\ \mathbf{F}\ (x_2, y_2)$ *then* $(x_2, y_2)\ \mathbf{F}\ (x_1, y_1)$*.]* Suppose (x_1, y_1) and (x_2, y_2) are elements of $\mathbf{R} \times \mathbf{R}$ such that $(x_1, y_1)\ \mathbf{F}\ (x_2, y_2)$. By definition of $\mathbf{F}$, this means that $x_1 = x_2$. By symmetry of equality, $x_2 = x_1$. Thus, by definition of $\mathbf{F}$, $(x_2, y_2)\ \mathbf{F}\ (x_1, y_1)$.

F is transitive: *[We must show that for all elements* (x_1, y_1), (x_2, y_2), *and* (x_3, y_3) *in* $\mathbf{R} \times \mathbf{R}$, *if* $(x_1, y_1)\ \mathbf{F}\ (x_2, y_2)$ *and* $(x_2, y_2)\ \mathbf{F}\ (x_3, y_3)$ *then* $(x_1, y_1)\ \mathbf{F}\ (x_3, y_3)$*.]* Suppose (x_1, y_1), (x_2, y_2), and (x_3, y_3) are elements of $\mathbf{R} \times \mathbf{R}$ such that $(x_1, y_1)\ \mathbf{F}\ (x_2, y_2)$ and $(x_2, y_2)\ \mathbf{F}\ (x_3, y_3)$. By definition of $\mathbf{F}$, this means that $x_1 = x_2$ and $x_2 = x_3$. By transitivity of equality, $x_1 = x_3$. Hence, by definition of $\mathbf{F}$, $(x_1, y_1)\ \mathbf{F}\ (x_3, y_3)$.

31. ***R is reflexive:*** R is reflexive $\Leftrightarrow$ for every person p in A, $p\ R\ p$. By definition of R, this means that for every person p living in the world today, p lives within 100 miles of p, which is true.

R is symmetric: *[We must show that for all people p and q in A, if p R q then q R p.]* Suppose p and q are people in A such that $p\ R\ q$. By definition of R, this means that p lives within 100 miles of q. This implies that q lives within 100 miles of p. So, by definition of R, $q\ R\ p$.

R is not transitive: R is transitive $\Leftrightarrow$ for all people p, q, and r, if $p\ R\ q$ and $q\ R\ r$ then $p\ R\ r$. This is false. As a counterexample, take p to be an inhabitant of Chicago, Illinois, q an inhabitant of Kankakee, Illinois, and r an inhabitant of Champaign, Illinois. Then $p\ R\ q$ because Chicago is less than 100 miles from Kankakee, and $q\ R\ r$ because Kankakee is less than 100 miles from Champaign, but $p \not R\ r$ because Chicago is not less than 100 miles from Champaign.

34. Proof: Suppose R is any reflexive relation on a set A. *[We must show that R^{-1} is reflexive. To show this, we must show that for every x in A, $x\ R^{-1}\ x$.]* Given any element x in A, since R is reflexive, $x\ R\ x$, and by definition of relation, this means that $(x, x) \in R$. It follows, by definition of the inverse of a relation, that $(x, x) \in R^{-1}$, and so, by definition of relation, $x\ R^{-1}\ x$ *[as was to be shown].*

37. a. ***R ∩ S is reflexive:*** Suppose R and S are reflexive. *[To show that $R \cap S$ is reflexive, we must show that $\forall x \in A$, $(x, x) \in R \cap S$.]* So suppose $x \in A$. Since R is reflexive, $(x, x) \in R$, and since S is reflexive, $(x, x) \in S$. Thus, by definition of intersection, $(x, x) \in R \cap S$ *[as was to be shown].*

38. *Hint:* The answer is yes.

41. Yes. To prove this we must show that for all x and y in A, if $(x, y) \in R \cup S$ then $(y, x) \in R \cup S$. So suppose (x, y) is a particular but arbitrarily chosen element in $R \cup S$. *[We must show that $(y, x) \in R \cup S$.]* By definition of union, $(x, y) \in R$ or $(x, y) \in S$. In case $(x, y) \in R$, then $(y, x) \in R$ because R is symmetric, and hence $(y, x) \in R \cup S$ by definition of union. In case $(x, y) \in S$ then $(y, x) \in S$ because S is symmetric, and hence $(y, x) \in R \cup S$ by definition of union. Thus, in both cases, $(y, x) \in R \cup S$ *[as was to be shown].*

43. R_1 is not irreflexive because $(0, 0) \in R_1$. R_1 is not asymmetric because $(0, 1) \in R_1$ and $(1, 0) \in R_1$. R_1 is not intransitive because $(0, 1) \in R_1$ and $(1, 0) \in R_1$ and $(0, 0) \in R_1$.

45. R_3 is irreflexive because no element of A is related by R_3 to itself. R_3 is not asymmetric because $(2, 3) \in R_3$ and $(3, 2) \in R_3$. R_3 is intransitive. To see why, observe that R_3 consists only of $(2, 3)$ and $(3, 2)$. Now $(2, 3) \in R_3$ and $(3, 2) \in R_3$ but $(2, 2) \notin R_3$. Also $(3, 2) \in R_3$ and $(2, 3) \in R_3$ but $(3, 3) \notin R_3$.

48. R_6 is irreflexive because no element of A is related by R_6 to itself. R_6 is asymmetric because R_6 consists only of $(0, 1)$ and $(0, 2)$ and neither $(1, 0)$ nor $(2, 0)$ is in R_6. R_6 is not intransitive. Let $x = y = z = 0$. Then $(x, y) \in R_6$ and $(y, z) \in R_6$ and $(x, z) \in R_6$.

51. $R^t = R \cup \{(0, 0), (0, 3), (1, 0), (3, 1), (3, 2), (3, 3), (0, 2), (1, 2)\}$
$= \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3), (2, 2), (3, 0), (3, 1), (3, 2), (3, 3)\}$

54. ***Algorithm—Test for Reflexivity***

[The input for this algorithm is a binary relation R defined on a set A, that is represented as the one-dimensional array a[1], a[2],…, a[n]. To test whether R is reflexive, a variable called answer is initially set equal to "yes," and each element a[i] of A is examined in turn to see whether it is related by R to itself. If any element is not related to itself by R, then answer is set equal to "no," the while loop is not repeated, and processing terminates.]

Input: *n [a positive integer], a[1], a[2], . . . , a[n] [a one-dimensional array representing a set A], R [a subset of A × A]*

Algorithm Body:

i := 1, *answer* := *"yes"*
while (*answer* = *"yes" and i* ≤ *n*)
  if (*a*[*i*], *a*[*i*]) ∉ *R* **then** *answer* := *"no"*
  i := *i* + 1
end while

Output: *answer [a string]*

SECTION 8.3

1. a. $c\ R\ c$ **b.** $b\ R\ a, c\ R\ b, e\ R\ d$ **c.** $a\ R\ c$
d. $c\ R\ c, b\ R\ a, c\ R\ b, e\ R\ d, a\ R\ c, c\ R\ a$

2. a. $R = \{(0, 0), (0, 2), (2, 0), (2, 2), (1, 1), (3, 3), (3, 4), (4, 3), (4, 4)\}$

3. $[0] = \{0, 4\}, [1] = \{1, 3\}, [2] = \{2\}, [3] = \{1, 3\}$
There are three distinct equivalence classes:
$[0] = \{0, 4\} = [4], [1] = \{1, 3\} = [3], [2] = \{2\}$

5. $[1] = \{1, 5, 9, 13, 17\}, [2] = \{2, 6, 10, 14, 18\}$,
$[3] = \{3, 7, 11, 15, 19\}, [4] = \{4, 8, 12, 16, 20\}$,
$[5] = \{5, 9, 13, 17, 1\} = [1]$
There are four distinct equivalence classes: [1], [2], [3], [4]

7. $\{(1, 3), (3, 9)\}, \{(2, 4), (-4, -8), (3, 6)\}, \{(1, 5)\}$

8. $\{\varnothing\}, \{\{a\}, \{b\}, \{c\}\}, \{\{a, b\}, \{a, c\}, \{b, c\}\}, \{\{a, b, c\}\}$

11. $[0] = \{x \in A \mid 4 \mid (x^2 - 0)\} = \{x \in A \mid 4 \mid x^2\}$
$= \{-4, -2, 0, 2, 4\}$
$[1] = \{x \in A \mid 4 \mid (x^2 - 1^2)\} = \{x \in A \mid 4 \mid (x^2 - 1)\}$
$= \{-3, -1, 1, 3\}$

13. {*aaaa*, *aaab*, *aaba*, *aabb*}, {*abaa*, *abab*, *abba*, *abbb*}, {*baaa*, *baab*, *baba*, *babb*}, {*bbaa*, *bbab*, *bbba*, *bbbb*}

15. a. True. $17 - 2 = 15$ and $5 \mid 15$.

16. a. $[7] = [4] = [19]$, $[-4] = [17]$, $[-6] = [27]$

17. a. Proof: Suppose that m and n are integers such that $m \equiv n \pmod 3$. *[We must show that* $m \bmod 3 = n \bmod 3$*.]* By definition of congruence, $3 \mid (m - n)$, and so, by definition of divisibility, $m - n = 3a$ for some integer a. Let $r = m \bmod 3$. Then $m = 3b + r$ for some integer b. Since $m - n = 3a$, it follows by substitution that $m - n = (3b + r) - n = 3a$, or, equivalently, $n = 3(b - a) + r$.
Now $b - a$ is an integer and $0 \le r < 3$. So, by definition of *mod*, $n \bmod 3 = r$, which equals $m \bmod 3$.
Suppose that m and n are integers such that $m \bmod 3 = n \bmod 3$. *[We must show that* $m \equiv n \pmod 3$*.]* Let $r = m \bmod 3 = n \bmod 3$. Then, by definition of *mod*, $m = 3p + r$ and $n = 3q + r$ for some integers p and q. By substitution, $m - n = (3p + r) - (3q + r) = 3(p - q)$. Since $p - q$ is an integer, it follows that $3 \mid (m - n)$, and so, by definition of congruence, $m \equiv n \pmod 3$.

18. a. *One possible answer:* Let $A = \{1, 2\}$ and $B = \{2, 3\}$. Then $A \neq B$, so A and B are distinct. But A and B are not disjoint since $2 \in A \cap B$.

19. a. (1) Proof: R is reflexive because it is true that for each student x at a college, x has the same major (or double major) as x.

R is symmetric because it is true that for all students x and y at a college, if x has the same major (or double major) as y, then y has the same major (or double major) as x.

R is transitive because it is true that for all students x, y, and z at a college, if x has the same major (or double major) as y and y has the same major (or double major) as z, then x has the same major (or double major) as z. R is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one equivalence class for each major and double major at the college. Each class consists of all students with that major (or double major).

20. (1) The solution to exercise 12 in Section 8.2 proved that E is reflexive, symmetric, and transitive. Thus E is an equivalence relation.

(2) Observe that for any integer a, the equivalence class of a is

$$\begin{aligned} [a] &= \{x \in \mathbf{Z} \mid xEa\} \\ &\qquad \text{by definition of equivalence class} \\ &= \{x \in \mathbf{Z} \mid x - a \text{ is divisible by } 4\} \\ &\qquad \text{by definition of } E \\ &= \{x \in \mathbf{Z} \mid x - a = 4k \text{ for some integer } k\} \\ &\qquad \text{by definition of divisibility} \\ &= \{x \in \mathbf{Z} \mid x = 4k + a \text{ for some integer } k\} \\ &\qquad \text{by algebra.} \end{aligned}$$

Now when any integer a is divided by 4, the only possible remainders are 0, 1, 2, and 3 and no integer has two distinct remainders when it is divided by 4. Thus every integer is contained in exactly one of the following four equivalence classes:

$$\{x \in Z \mid x = 4k \text{ for some integer } k\}$$
$$\{x \in Z \mid x = 4k + 1 \text{ for some integer } k\}$$
$$\{x \in Z \mid x = 4k + 2 \text{ for some integer } k\}$$
$$\{x \in Z \mid x = 4k + 3 \text{ for some integer } k\}$$

21. *Hint:* Use facts about even and odd integers from Section 4.2 to show that $m \, R \, n$, if, and only if, m and n are both even or m and n are both odd, or, in other words, if, and only if, both m and n have the same parity. Use that result to show that R is an equivalence relation with two distinct equivalence classes: the set of all even integers and the set of all odd integers.

25. (1) Proof: A is reflexive because each real number has the same absolute value as itself.

A is symmetric because for all real numbers x and y, if $|x| = |y|$ then $|y| = |x|$.

A is transitive because for all real numbers x, y, and z, if $|x| = |y|$ and $|y| = |z|$ then $|x| = |z|$.

A is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) The distinct classes are all sets of the form $\{x, -x\}$, where x is a real number.

26. *Hints*: (1) D is reflexive, symmetric, and transitive. The proofs are very similar to the proofs in exercise 17.

(2) There are two distinct equivalence classes. Note that $m^2 - n^2 = (m - n)(m + n)$ for all integers m and n. In addition, $3 \mid (m - n)$ or $3 \mid (m + n) \Leftrightarrow$ either $m - n = 3r$ or $m + n = 3r$, for some integer r.

28. (1) Proof: I is reflexive because the difference between each real number and itself is 0, which is an integer.

I is symmetric because for all real numbers x and y, if $x - y$ is an integer, then $y - x = (-1)(x - y)$, which is also an integer.

I is transitive because for all real numbers x, y, and z, if $x - y$ is an integer and $y - z$ is an integer, then $x - z = (x - y) + (y - z)$ is the sum of two integers and thus is an integer.

I is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one class for each real number x with $0 \le x < 1$. The distinct classes are all sets of the form $\{y \in \mathbf{R} \mid y = n + x$, for some integer $n\}$, where x is a real number such that $0 \le x < 1$.

29. (1) Proof: P is reflexive because each ordered pair of real numbers has the same first element as itself.

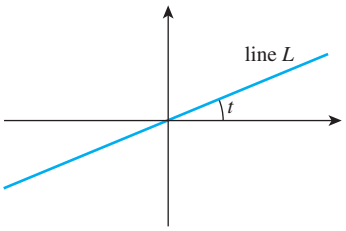
P is symmetric for the following reason: Suppose (w, x) and (y, z) are ordered pairs of real numbers such that $(w, x)\ P\ (y, z)$. Then, by definition of P, $w = y$. Now by the symmetric property of equality, this implies that $y = w$, and so, by definition of P, $(y, z)\ P\ (w, x)$.

P is transitive for the following reason: Suppose (u, v), (w, x), and (y, z) are ordered pairs of real numbers such that $(u, v)\ P\ (w, x)$ and $(w, x)\ P\ (y, z)$. Then, by definition of P, $u = w$ and $w = y$. It follows from the transitive property of equality that $u = y$. Hence, by definition of P, $(u, v)\ P\ (y, z)$.

P is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one equivalence class for each real number. The distinct equivalence classes are all sets of ordered pairs $\{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = a\}$, for each real number a. Equivalently, the equivalence classes consist of all vertical lines in the Cartesian plane.

32. *Solution:* There is one equivalence class for each real number t such that $0 \le t < \pi$. One line in each class goes through the origin, and that line makes an angle of t with the positive horizontal axis.



Alternatively, there is one equivalence class for every possible slope: all real numbers plus "undefined."

34. No. If points p, q, and r all lie on a straight line with q in the middle, and if p is c units from q and q is c units from r, then p is more than c units from r.

36. Proof: Suppose R is an equivalence relation on a set A and $a \in A$. Because R is an equivalence relation, R is reflexive, and because R is reflexive, each element of A is related to itself by R. In particular, $a\ R\ a$. Hence, by definition of equivalence class, $a \in [a]$.

38. Proof: Suppose R is an equivalence relation on a set A and a, b, and c are elements of A with $b\ R\ c$ and $c \in [a]$. Since $c \in [a]$, then $c\ R\ a$ by definition of equivalence class. Now R is transitive because R is an equivalence relation. Thus, since $b\ R\ c$ and $c\ R\ a$, then $b\ R\ a$. It follows that $b \in [a]$ by definition of equivalence class.

40. Proof: Suppose a, b, and x are in A, $a\ R\ b$, and $x \in [a]$. By definition of equivalence class, $x\ R\ a$. So $x\ R\ a$ and $a\ R\ b$, and thus, by transitivity, $x\ R\ b$. Hence $x \in [b]$.

41. *Hint:* To show that $[a] = [b]$, show that $[a] \subseteq [b]$ and $[b] \subseteq [a]$. To show that $[a] \subseteq [b]$, show that for every x in A, if $x \in [a]$ then $x \in [b]$.

42. c. *One possible answer:* $(2, 6)$, $(-2, -6)$, $(3, 9)$, $(-3, -9)$.

43. a. Suppose that (a, b), (a', b'), (c, d), and (c', d') are any elements of A such that

$$[(a, b)] = [(a', b')] \text{ and } [(c, d)] = [(c', d')].$$

By definition of R,

$$ab' = ba' \text{ (*) and } cd' = dc' \text{ (**)}.$$

We must show that

$$[(a, b)] + [(c, d)] = [(a', b')] + [(c', d')].$$

By definition of the addition on A, this equation is true if, and only if,

$$[(ad + bc, bd)] = [(a'd' + b'c', b'd')].$$

And, by definition of the relation, this equation is true if, and only if,

$$(ad + bc)b'd' = bd(a'd' + b'c').$$

After multiplying out, this becomes

$$adb'd' + bcb'd' = bda'd' + bdb'c',$$

and regrouping, turns it into

$$(ab')(dd') + (cd')(bb') = (ba')(dd') + (dc')(bb').$$

Substituting the values from (*) and (**) shows that this last equation is true.

c. Suppose that (a, b) is any element of A. We must show that

$$[(a, b)] + [(0, 1)] = [(a, b)].$$

By definition of the addition on A, this equation is true if, and only if,

$$[(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a, b)].$$

And this last equation is true because $a \cdot 1 + b \cdot 0 = a$ and $b \cdot 1 = b$.

e. Suppose that (a, b) is any element of A. We must show that

$$[(a, b)] + [(-a, b)] = [(-a, b)] + [(a, b)] = [(0, 1)].$$

By definition of the addition on A, this equation is true if, and only if,

$$[(ab + b(-a), bb)] = [(0, 1)],$$

or, equivalently,

$$[(0, bb)] = [(0, 1)].$$

By definition of the relation, this last equation is true if, and only if, $0 \cdot 1 = bb \cdot 0$, which is true.

44. a. Let (a, b) be any element of $\mathbf{Z}^+ \times \mathbf{Z}^+$. We must show that $(a, b)\ R\ (a, b)$. By definition of R, this relationship holds if, and only if, $a + b = b + a$. But this equation is true by the commutative law of addition for real numbers. Hence R is reflexive.

c. *Hint:* You will need to show that for any positive integers a, b, c, and d, if $a + d = c + b$ and $c + f = d + e$, then $a + f = b + e$.

d. *One possible answer:* (1, 1), (2, 2), (3, 3), (4, 4), (5, 5)

g. Observe that for any positive integers a and b, the equivalence class of (a, b) consists of all ordered pairs in $\mathbf{Z}^+ \times \mathbf{Z}^+$ for which the difference between the first and second coordinates equals $a - b$. Thus there is one equivalence class for each integer: positive, negative, and zero. Each positive integer n corresponds to the class of $(n + 1, 1)$; each negative integer $-n$ corresponds to the class of $(1, n + 1)$; and zero corresponds to the class $(1, 1)$.

47. c. "Ways and Means"

SECTION 8.4

1. a. ZKHUH VKDOO ZH PHHW

b. IN THE CAFETERIA

3. a. The relation $3 \mid (25 - 19)$ is true because $25 - 19 = 6$ and $3 \mid 6$ (since $6 = 3 \cdot 2$).

b. By definition of congruence modulo n, to show that $25 \equiv 19 \pmod 3$, one must show that $3/(25 - 19)$. This was verified in part (a).

c. To show that $25 = 19 + 3k$ for some integer k, one solves the equation for k and checks that the result is an integer. In this case, $k = (25 - 19)/3 = 2$, which is an integer. Thus $25 = 19 + 2 \cdot 3$.

d. When 25 is divided by 3, the remainder is 1 because $25 = 3 \cdot 8 + 1$. When 19 is divided by 3, the remainder is also 1 because $19 = 3 \cdot 6 + 1$. Thus 25 and 19 have the same remainder when divided by 3.

e. By definition, $25\ mod\ 3$ is the remainder obtained when 25 is divided by 3, and $19\ mod\ 3$ is the remainder obtained when 19 is divided by 3. In part (d) these two numbers were shown to be equal.

6. *Hints:* (1) Use the quotient-remainder theorem and Theorem 8.4.1 to show that given any integer a, a is in one of the classes $[0], [1], [2], \ldots [n - 1]$. (2) Use the quotient-remainder theorem (Theorem 4.5.1) to prove that if $0 \le a < n$, $0 \le b < n$, and $a \equiv b \pmod n$, then $a = b$.

7. a. $128 \equiv 2 \pmod 7$ because $128 - 2 = 126 = 7 \cdot 18$, and $61 \equiv 5 \pmod 7$ because $61 - 5 = 56 = 7 \cdot 8$

b. $128 + 61 \equiv (2 + 5) \pmod 7$ because $128 + 61 = 189$, $2 + 5 = 7$, and $189 - 7 = 182 = 7 \cdot 26$

c. $128 - 61 \equiv (2 - 5) \pmod 7$ because $128 - 61 = 67$, $2 - 5 = -3$, and $67 - (-3) = 70 = 7 \cdot 10$

d. $128 \cdot 61 \equiv (2 \cdot 5) \pmod 7$ because $128 \cdot 61 = 7808$, $2 \cdot 5 = 10$, and $7808 - (10) = 7798 = 7 \cdot 1114$

e. $128^2 \equiv 2^2 \pmod 7$ because $128^2 = 16384$, $2^2 = 4$, and $16384 - 4 = 16380 = 7 \cdot 2340$.

9. a. Proof: Suppose a, b, c, d, and n are integers with $n > 1$, $a \equiv c \pmod n$, and $b \equiv d \pmod n$. By Theorem 8.4.1, $a - c = nr$ and $b - d = ns$ for some integers r and s. Then

$$\begin{aligned}(a + b) - (c + d) &= (a - c) + (b - d) = nr + ns \\ &= n(r + s).\end{aligned}$$

Now $r + s$ is an integer, and so, by Theorem 8.4.1, $a + b \equiv (c + d) \pmod n$.

12. a. Proof (by mathematical induction): Let the property $P(n)$ be the congruence $10^n \equiv 1 \pmod 9$.

Show that P(0) is true:

When $n = 0$, the left-hand side of the congruence is $10^0 = 1$ and the right-hand side is also 1.

Show that for every integer k ≥ 0, if P(k) is true, then P(k + 1) is true.

Let k be any integer with $k \ge 0$, and suppose $P(k)$ is true. That is, suppose $10^k \equiv 1 \pmod 9$. (*) *[This is the inductive hypothesis.]* By Theorem 8.4.1, $10 \equiv 1 \pmod 9$ (**) because $10 - 1 = 9 = 9 \cdot 1$. And by Theorem 8.4.3, we can multiply the left- and right-hand sides of (*) and (**) to obtain $10^k \cdot 10 \equiv 1 \cdot 1 \pmod 9$, or, equivalently, $10^{k+1} \equiv 1 \pmod 9$. Hence $P(k + 1)$ is true.

Alternative Proof: Note that $10 \equiv 1 \pmod 9$ because $10 - 1 = 9$ and $9 \mid 9$. Thus by Theorem 8.4.3(4), $10^n \equiv 1^n \equiv 1 \pmod 9$.

14. $14^1\ mod\ 55 = 14$

$14^2\ mod\ 55 = 196\ mod\ 55 = 31$

$14^4\ mod\ 55 = (14^2\ mod\ 55)^2\ mod\ 55 = 31^2\ mod\ 55 = 26$

$14^8\ mod\ 55 = (14^4\ mod\ 55)^2\ mod\ 55 = 26^2\ mod\ 55 = 16$

$14^{16}\ mod\ 55 = (14^8\ mod\ 55)^2\ mod\ 55 = 16^2\ mod\ 55 = 36$

15. $4^{27}\ mod\ 55 = 14^{16+8+2+1}\ mod\ 55$

$= \{(14^{16}\ mod\ 55)(14^8\ mod\ 55)(14^2\ mod\ 55)(14^1\ mod\ 55)\}\ mod\ 55$

$= (36 \cdot 16 \cdot 31 \cdot 14)\ mod\ 55 = 249984\ mod\ 55 = 9$

16. Note that $307 = 256 + 32 + 16 + 2 + 1$.

$675^1 \ mod\ 713 = 675$

$675^2 \ mod\ 713 = 18$

$675^4 \ mod\ 713 = 18^2 \ mod\ 713 = 324$

$675^8 \ mod\ 713 = 324^2 \ mod\ 713 = 165$

$675^{16} \ mod\ 713 = 165^2 \ mod\ 713 = 131$

$675^{32} \ mod\ 713 = 131^2 \ mod\ 713 = 49$

$675^{64} \ mod\ 713 = 49^2 \ mod\ 713 = 262$

$675^{128} \ mod\ 713 = 262^2 \ mod\ 713 = 196$

$675^{256} \ mod\ 713 = 196^2 \ mod\ 713 = 627$

Thus

$$675^{307} \ mod\ 713 = 675^{256+32+16+2+1} \ mod\ 713$$
$$= (675^{256} \cdot 675^{32} \cdot 675^{16} \cdot 675^2 \cdot 675^1) \ mod\ 713$$
$$= (627 \cdot 49 \cdot 131 \cdot 18 \cdot 675) \ mod\ 713 = 3.$$

19. The letters in HELLO translate numerically into 08, 05, 12, 12, and 15. By Example 8.4.9, the H is encrypted as 17. To encrypt E, we compute $5^3 \ mod\ 55 = 15$. To encrypt L, we compute $12^3 \ mod\ 55 = 23$. And to encrypt O, we compute $15^3 \ mod\ 55 = 20$. Thus the ciphertext is 17 15 23 23 20. (In practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.)

22. By Example 8.4.10, the decryption key is 27. Thus the residues modulo 55 for 13^{27}, 20^{27}, and 9^{27} must be found and then translated into letters of the alphabet.

Because $27 = 16 + 8 + 2 + 1$, we first perform the following computations:

$13^1 \equiv 13 \pmod{55}$ $\quad$ $20^1 \equiv 20 \pmod{55}$

$13^2 \equiv 4 \pmod{55}$ $\quad$ $20^2 \equiv 15 \pmod{55}$

$13^4 \equiv 4^2 \equiv 16 \pmod{55}$ $\quad$ $20^4 \equiv 15^2 \equiv 5 \pmod{55}$

$13^8 \equiv 16^2 \equiv 36 \pmod{55}$ $\quad$ $20^8 \equiv 25^2 \equiv 5 \pmod{55}$

$13^{16} \equiv 36^2 \equiv 31 \pmod{55}$ $\quad$ $20^{16} \equiv 25^2 \equiv 20 \pmod{55}$

$$9^1 \equiv 9 \pmod{55}$$
$$9^2 \equiv 26 \pmod{55}$$
$$9^4 \equiv 26^2 \equiv 16 \pmod{55}$$
$$9^8 \equiv 16^2 \equiv 36 \pmod{55}$$
$$9^{16} \equiv 36^2 \equiv 31 \pmod{55}$$

Then we compute

$13^{27} \ mod\ 55 = (31 \cdot 36 \cdot 4 \cdot 13) \ mod\ 55 = 7,$

$20^{27} \ mod\ 55 = (20 \cdot 25 \cdot 15 \cdot 20) \ mod\ 55 = 15,$

$9^{27} \ mod\ 55 = (31 \cdot 36 \cdot 26 \cdot 9) \ mod\ 55 = 4.$

Finally, because 7, 15, and 4 translate into letters as G, O, and D, we see that the message is GOOD.

25. *Hint:* By Theorem 5.2.2, using a in place of r and $n-1$ in place of n, we have $1 + a + a^2 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$.

Multiplying both sides by $a - 1$ gives

$$a^n - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{n-1}).$$

26. **Step 1:** $6664 = 765 \cdot 8 + 544$, and so $544 = 6664 - 765 \cdot 8$

Step 2: $765 = 544 \cdot 1 + 221$, and so $221 = 765 - 544$

Step 3: $544 = 221 \cdot 2 + 102$, and so $102 = 544 - 221 \cdot 2$

Step 4: $221 = 102 \cdot 2 + 17$, and so $17 = 221 - 102 \cdot 2$

Step 5: $102 = 17 \cdot 6 + 0$

Thus gcd(6664, 765) = 17 (which is the remainder obtained just before the final division). Substitute back through steps 4–1 to express 17 as a linear combination of 6664 and 765:

$$17 = 221 - 102 \cdot 2$$
$$= 221 - (544 - 221 \cdot 2) = 221 \cdot 5 - 544 \cdot 2$$
$$= (765 - 544) \cdot 5 - 544 \cdot 2 = 765 \cdot 5 - 544 \cdot 7$$
$$= 765 \cdot 5 - (6664 - 765 \cdot 8) \cdot 7 = (-7) \cdot 6664 + 61 \cdot 765.$$

(When you have finished this final step, it is wise to verify that you have not made a mistake by checking that the final expression really does equal the greatest common divisor.)

28.

a	330	156	18	12	6
b	156	18	12	6	0
r		18	12	6	0
q		2	8	1	2
s	1	0	1	−8	9
t	0	1	−2	17	−19
u	0	1	−8	9	−26
v	1	−2	17	−19	55
$newu$		1	−8	9	−26
$newv$		−2	17	−19	55
$sa + tb$	330	18	−6	6	6

31. **a.** **Step 1:** $210 = 13 \cdot 16 + 2$, and so $2 = 210 - 16 \cdot 13$

Step 2: $13 = 2 \cdot 6 + 1$, and so $1 = 13 - 2 \cdot 6$

Step 3: $6 = 1 \cdot 6 + 0$, and so gcd(210, 13) = 1

Substitute back through steps 2 and 1:

$$1 = 13 - 2 \cdot 6$$
$$= 13 - (210 - 16 \cdot 13) \cdot 6 = (-6) \cdot 210 + 97 \cdot 13$$

Thus $210 \cdot (-6) \equiv 1 \pmod{13}$, and so -6 is an inverse for 210 modulo 13.

b. Compute $13 - 6 = 7$. Note that $7 \equiv -6 \pmod{13}$ because $7 - (-6) = 13 = 13 \cdot 1$. Thus, by Theorem 8.4.3(3), $210 \cdot 7 \equiv 210 \cdot (-6) \pmod{13}$. By part (a), -6 is an inverse for 210 modulo 13, and so $210 \cdot (-6) \equiv 1$

(mod 13). It follows, by the symmetric and transitive properties of congruence, that $210 \cdot 7 \equiv 1 \pmod{13}$, and so 7 is a positive inverse for 210 modulo 13.

c. This problem can be solved using either the result of part (a) or that of part (b). By part (b) $210 \cdot 7 \equiv 1 \pmod{13}$. Multiply both sides by 8 and apply Theorem 8.4.3(3) to obtain $210 \cdot 56 \equiv 8 \pmod{13}$. Thus a positive solution for $210x \equiv 8 \pmod{13}$ is $x = 56$. Note that the least positive residue corresponding to this solution is also a solution. By Theorem 8.4.1, $56 \equiv 4 \pmod{13}$ because $56 = 13 \cdot 4 + 4$, and so, by Theorem 8.4.3(3), $210 \cdot 56 \equiv 210 \cdot 4 \equiv 9 \pmod{13}$. This shows that 4 is also a solution for the congruence, and because $0 \leq 4 < 13$, 4 is the least positive solution for the congruence.

33. *Hint:* If $as + bt = 1$ and $c = au = bv$, then $c = asc + btc = as(bv) + bt(au)$.

35. Proof: Let a be any integer and let n be any positive integer, and suppose s and t are any inverses for a modulo n. Thus $as \equiv 1 \pmod{n}$ and $at \equiv 1 \pmod{n}$. Note that $ast = (as) \cdot t = (at) \cdot s$ By Theorem 8.4.3(3), $(as) \cdot t \equiv t \pmod{n}$ and $(at) \cdot s \equiv s \pmod{n}$. Thus, by symmetry and transitivity of congruence modulo n, $s \equiv t \pmod{n}$. Because s and t were chosen arbitrarily, we conclude that any two inverses for a are congruent modulo n.

36. The numeric equivalents of H, E, L, and P are 08, 05, 12, and 16. To encrypt these letters, the following quantities must be computed: $8^{43} \; mod \; 713$, $5^{43} \; mod \; 713$, $12^{43} \; mod \; 713$, and $16^{43} \; mod \; 713$. We use the fact that $43 = 32 + 8 + 2 + 1$.

H: $8 \equiv 8 \pmod{713}$
$8^2 \equiv 64 \pmod{713}$
$8^4 \equiv 64^2 \equiv 531 \pmod{713}$
$8^8 \equiv 531^2 \equiv 326 \pmod{713}$
$8^{16} \equiv 326^2 \equiv 39 \pmod{713}$
$8^{32} \equiv 39^2 \equiv 95 \pmod{713}$
Thus the ciphertext is
$8^{43} \; mod \; 713$
$= (95 \cdot 326 \cdot 64 \cdot 8) \; mod \; 713 = 233.$

E: $5 \equiv 5 \pmod{713}$
$5^2 \equiv 25 \pmod{713}$
$5^4 \equiv 625 \pmod{713}$
$5^8 \equiv 625^2 \equiv 614 \pmod{713}$
$5^{16} \equiv 614^2 \equiv 532 \pmod{713}$
$5^{32} \equiv 532^2 \equiv 676 \pmod{713}$
Thus the ciphertext is
$8^{43} \; mod \; 713$
$= (676 \cdot 614 \cdot 25 \cdot 5) \; mod \; 713 = 129.$

L: $12 \equiv 12 \pmod{713}$
$12^2 \equiv 144 \pmod{713}$
$12^4 \equiv 144^2 \equiv 59 \pmod{713}$
$12^8 \equiv 59^2 \equiv 629 \pmod{713}$
$12^{16} \equiv 629^2 \equiv 639 \pmod{713}$
$12^{32} \equiv 639^2 \equiv 485 \pmod{713}$
Thus the ciphertext is
$12^{43} \; mod \; 713$
$= (485 \cdot 629 \cdot 144 \cdot 12) \; mod \; 713 = 48.$

P: $16 \equiv 16 \pmod{713}$
$16^2 \equiv 256 \pmod{713}$
$16^4 \equiv 256^2 \equiv 653 \pmod{713}$
$16^8 \equiv 653^2 \equiv 35 \pmod{713}$
$16^{16} \equiv 35^2 \equiv 512 \pmod{713}$
$16^{32} \equiv 512^2 \equiv 473 \pmod{713}$
Thus the ciphertext is
$16^{43} \; mod \; 713$
$= (473 \cdot 35 \cdot 256 \cdot 16) \; mod \; 713 = 128.$

Therefore, the encrypted message is 233 129 048 128. (Again, note that in practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words. We kept them separate so that the numbers in the computations would be smaller and easier to work with.)

39. By exercise 38, the decryption key, d, is 307. Hence, to decrypt the message, the following quantities must be computed: $675^{307} \; mod \; 713$, $89^{307} \; mod \; 713$, and $48^{307} \; mod \; 713$. We use the fact that $307 = 256 + 32 + 16 + 2 + 1$.

$675 \equiv 675 \pmod{713}$
$675^2 \equiv 18 \pmod{713}$
$675^4 \equiv 18^2 \equiv 324 \pmod{713}$
$675^8 \equiv 324^2 \equiv 165 \pmod{713}$
$675^{16} \equiv 165^2 \equiv 131 \pmod{713}$
$675^{32} \equiv 131^2 \equiv 49 \pmod{713}$
$675^{64} \equiv 49^2 \equiv 262 \pmod{713}$
$675^{128} \equiv 262^2 \equiv 196 \pmod{713}$
$675^{256} \equiv 196^2 \equiv 627 \pmod{713}$

$89 \equiv 89 \pmod{713}$
$89^2 \equiv 78 \pmod{713}$
$89^4 \equiv 78^2 \equiv 380 \pmod{713}$
$89^8 \equiv 380^2 \equiv 374 \pmod{713}$
$89^{16} \equiv 374^2 \equiv 128 \pmod{713}$
$89^{32} \equiv 128^2 \equiv 698 \pmod{713}$
$89^{64} \equiv 698^2 \equiv 225 \pmod{713}$
$89^{128} \equiv 225^2 \equiv 2 \pmod{713}$
$89^{256} \equiv 2^2 \equiv 4 \pmod{713}$

$48 \equiv 48 \pmod{713}$
$48^2 \equiv 165 \pmod{713}$
$48^4 \equiv 131 \pmod{713}$
$48^8 \equiv 49 \pmod{713}$
$48^{16} \equiv 262 \pmod{713}$
$48^{32} \equiv 196 \pmod{713}$
$48^{64} \equiv 627 \pmod{713}$
$48^{128} \equiv 627^2 \equiv 266 \pmod{713}$
$48^{256} \equiv 266^2 \equiv 169 \pmod{713}$

Thus the decryption for 675 is

$$675^{307} \bmod 713 = (675^{256+32+16+2+1}) \bmod 713$$
$$= (627 \cdot 49 \cdot 131 \cdot 18 \cdot 675) \bmod 713 = 3,$$

which corresponds to the letter *C*.

The decryption for 89 is

$$89^{307} \bmod 713 = (89^{256+32+16+2+1}) \bmod 713$$
$$= (4 \cdot 698 \cdot 128 \cdot 78 \cdot 89) \bmod 713 = 15,$$

which corresponds to the letter *O*.

The decryption for 48 is

$$48^{307} \bmod 713 = (48^{256+32+16+2+1}) \bmod 713$$
$$= (169 \cdot 196 \cdot 262 \cdot 165 \cdot 48) \bmod 713 = 12,$$

which corresponds to the letter *L*.

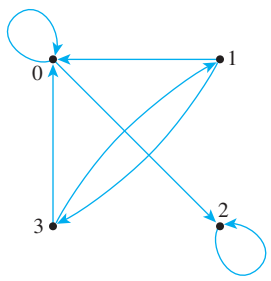
Thus the decrypted message is COOL.

41. a. *Hint:* For the inductive step, assume $p \mid q_1 q_2 \cdots q_{s+1}$ and let $a = q_1 q_2 \cdots q_s$. Then $p \mid a q_{s+1}$, and either $p = q_{s+1}$ or Euclid's lemma and the inductive hypothesis can be applied.

42. a. When $a = 15$ and $p = 7$, $a^{p-1} = 15^6 = 11390625 \equiv 1 \pmod 7$ because $11390625 - 1 = 7 \cdot 1627232$.

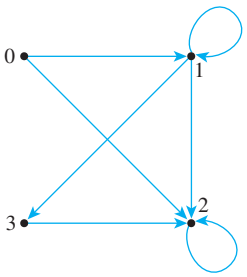
SECTION 8.5

1. a.



R_1 is not antisymmetric: $1\ R_1\ 3$ and $3\ R_1\ 1$ and $1 \neq 3$.

b.



R_2 is antisymmetric: There are no cases where $a\ R\ b$ and $b\ R\ a$ and $a \neq b$.

2. R is not antisymmetric. Let x and y be any two distinct people of the same age. Then $x\ R\ y$ and $y\ R\ x$ but $x \neq y$.

5. R is a partial order relation.

Proof:

R is reflexive: Suppose $(a, b) \in \mathbf{R} \times \mathbf{R}$. Then $(a, b)\ R\ (a, b)$ because $a = a$ and $b \leq b$.

R is antisymmetric: Suppose (a, b) and (c, d) are ordered pairs of real numbers such that $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (a, b)$. Then

$$\text{either } a < c \quad \text{or} \quad \text{both } a = c \text{ and } b \leq d$$

and

$$\text{either } c < a \quad \text{or} \quad \text{both } c = a \text{ and } d \leq b.$$

Thus

$$a \leq c \text{ and } c \leq a$$

and so

$$a = c.$$

Consequently,

$$b \leq d \quad \text{and} \quad d \leq b$$

and so

$$b = d.$$

Hence $(a, b) = (c, d)$.

R is transitive: Suppose (a, b), (c, d), and (e, f) are ordered pairs of real numbers such that $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (e, f)$. Then

$$\text{either } a < c \quad \text{or} \quad \text{both } a = c \text{ and } b \leq d$$

and

$$\text{either } c < e \quad \text{or} \quad \text{both } c = e \text{ and } d \leq f.$$

It follows that one of the following cases must occur.

Case 1 ($a < c$ and $c < e$): Then by transitivity of $<$, $a < e$, and so $(a, b)\ R\ (e, f)$ by definition of R.

Case 2 ($a < c$ and $c = e$): Then by substitution, $a < e$, and so $(a, b)\ R\ (e, f)$ by definition of R.

Case 3 ($a = c$ and $c < e$): Then by substitution, $a < e$, and so $(a, b)\ R\ (e, f)$ by definition of R.

***Case 4* ($a = c$ *and* $c = e$):** Then by definition of R, $b \preceq d$ and $d \preceq f$, and so by transitivity of $\preceq$, $b \preceq f$. Hence $a = e$ and $b \preceq f$, and so $(a, b)\ R\ (e, f)$ by definition of R.

In each case, $(a, b)\ R\ (e, f)$. Therefore, R is transitive. Since R is reflexive, antisymmetric, and transitive, R is a partial order relation.

8. R is not a partial order relation because R is not antisymmetric.

Counterexample: $1\ R\ 3$ (because $1 + 3$ is even) and $3\ R\ 1$ (because $3 + 1$ is even) but $1 \neq 3$.

10. No. Counterexample: Define relations R and S on the set $\{1, 2\}$ as follows: $R = \{(1, 2)\}$ and $S = \{(2, 1)\}$. Then both R and S are antisymmetric, but $R \cup S = \{(1, 2), (2, 1)\}$ is not antisymmetric because $(1, 2) \in R \cup S$ and $(2, 1) \in R \cup S$ but $1 \neq 2$.

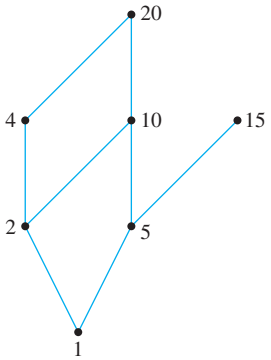
11. a. True, by (1).
b. False. By (1), $bba \preceq bbab$.

13. $R_1 = \{(a, a), (b, b)\}$, $R_2 = \{(a, a), (b, b), (a, b)\}$, $R_3 = \{(a, a), (b, b), (b, a)\}$

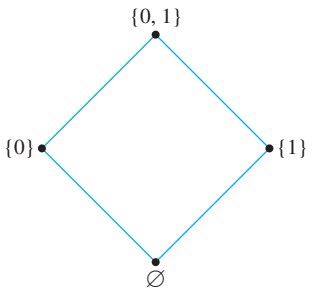
14. a. $R_1 = \{(a, a), (b, b), (c, c)\}$
$R_2 = \{(a, a), (b, b), (c, c), (b, a)\}$
$R_3 = \{(a, a), (b, b), (c, c), (c, a)\}$
$R_4 = \{(a, a), (b, b), (c, c), (b, a), (c, a)\}$
$R_5 = \{(a, a), (b, b), (c, c), (c, b), (c, a)\}$
$R_6 = \{(a, a), (b, b), (c, c), (b, c), (b, a)\}$
$R_7 = \{(a, a), (b, b), (c, c), (c, b), (b, a), (c, a)\}$
$R_8 = \{(a, a), (b, b), (c, c), (b, c), (b, a), (c, a)\}$
$R_9 = \{(a, a), (b, b), (c, c), (b, c)\}$
$R_{10} = \{(a, a), (b, b), (c, c), (c, b)\}$

15. *Hint:* R is the identity relation on A: $x\ R\ x$ for each $x \in A$, and $x \not R\ y$ if $x \neq y$.

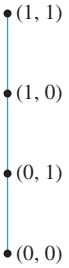
16. a.



17. a.



18.



21. a. Proof: *[We must show that for all a and b in A, $a \mid b$ or $b \mid a$.]* Let a and b be particular but arbitrarily chosen elements of A. By definition of A, there are nonnegative integers r and s such that $a = 2^r$ and $b = 2^s$. Now either $r \leq s$ or $s < r$. If $r \leq s$, then

$$b = 2^s = 2^r \cdot 2^{s-r} = a \cdot 2^{s-r},$$

where $s - r \geq 0$. It follows, by definition of divisibility, that $a \mid b$. By a similar argument, if $s < r$, then $b \mid a$. Hence either $a \mid b$ or $b \mid a$ *[as was to be shown].*

b.

22. greatest element: none; least element: 1; maximal elements: 15, 20; minimal element: 1

24. greatest element: $\{0, 1\}$; least element: $\varnothing$; maximal element: $\{0, 1\}$; minimal element: $\varnothing$

26. greatest element: (1, 1); least element: (0, 0); maximal element: (1, 1); minimal element: (0, 0)

30. a. No greatest element, no least element
b. Least element is 0, greatest element is 1

31. R is a total order relation because it is reflexive, antisymmetric, and transitive (so it is a partial order) and because $[b, a, c, d]$ is a chain that contains every element of A: $b\ R\ c$, $c\ R\ a$, and $a\ R\ d$.

34. *Hint:* Let R' be the restriction of R to B and show that R' is reflexive, antisymmetric, and transitive. In each case, this follows almost immediately from the fact that R is reflexive, antisymmetric, and transitive.

35. *One possible solution:* $\varnothing \subseteq \{w\} \subseteq \{w, x\} \subseteq \{w, x, y\} \subseteq \{w, x, y, z\}$

38. Proof: Suppose A is a partially ordered set with respect to a relation $\preceq$. By definition of total order, A is totally ordered if, and only if, any two elements of A are comparable. By definition of chain, this is true if, and only if, A is a chain.

39. Proof (by mathematical induction): Let A be a set that is totally ordered with respect to a relation $\preceq$, and let the property $P(n)$ be the sentence "Every subset of A with n elements has both a least element and a greatest element."

Show that P(1) is true:

If $A = \varnothing$, then $P(1)$ is true by default. So assume that A has at least one element, and suppose $S = \{a_1\}$ is a subset of A with one element. Because $\preceq$ is reflexive, $a_1 \preceq a_1$. So, by definition of least element and greatest element, a_1 is both a least element and a greatest element of S, and thus the property is true for $n = 1$.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

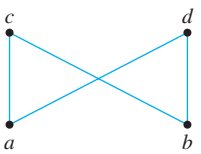
Let k be any integer with $k \geq 1$, and suppose that any subset of A with k elements has both a least element and a greatest element. *[Inductive hypothesis.]* We must show that any subset of A with $k+1$ elements has both a least element and a greatest element. If A has fewer than $k+1$ elements, then the statement is true by default. So assume that A has at least $k+1$ elements and that $S = \{a_1, a_2, \ldots, a_{k+1}\}$ is a subset of A with $k+1$ elements. By inductive hypothesis, $S - \{a_{k+1}\}$ has both a least element s and a greatest element t. Now because A is totally ordered, a_{k+1} and s are comparable. If $a_{k+1} \preceq s$, then, by transitivity of $\preceq$, a_{k+1} is the least element of S; otherwise, s remains the least element of S. And if $t \preceq a_{k+1}$, then, by transitivity of $\preceq$, a_{k+1} is the greatest element of S; otherwise, t remains the greatest element of S. Thus S has both a greatest element and a least element *[as was to be shown].*

40. a. Proof by contradiction: Suppose not. Suppose A is a nonempty, finite set that is partially ordered with respect to a relation $\preceq$, and suppose no element of A is minimal. Construct a sequence of elements x_1, x_2, x_3, … of A as follows:

1. Pick any element of A and call it x_1.
2. For each $i = 2, 3, 4, \ldots$, pick x_i to be an element of A for which $x_i \preceq x_{i-1}$ and $x_i \neq x_{i-1}$. *[Such an element must exist because otherwise x_{i-1} would be minimal, and we are supposing that no element of A is minimal.]* Now $x_i \neq x_j$ for any $i \neq j$. *[For if $x_i = x_j$, where $i < j$, then on the one hand, $x_j \preceq x_{j-1} \preceq \cdots \preceq x_{i+1} \preceq x_i$ and so $x_j \preceq x_{i+1}$. On the other hand, since $x_i = x_j$ and $x_i \succeq x_{i+1}$, then $x_j \succeq x_{i+1}$. Hence by antisymmetry, $x_j = x_{i+1}$, and so $x_i = x_{i+1}$ because $x_i = x_j$. But this contradicts the definition of the sequence $x_1, x_2, x_3, \ldots$]*

Thus $x_1, x_2, x_3, \ldots$ is an infinite sequence of distinct elements, and consequently $\{x_1, x_2, x_3, \ldots\}$ is an infinite subset of the finite set A, which is impossible. Hence the supposition is false and we conclude that any partially ordered subset of a finite set has a minimal element.

42.



44. One such total order is 1, 5, 2, 15, 10, 4, 20.

46. One such total order is (0, 0), (1, 0), (0, 1), (1, 1).

50. a. *One possible answer:* 1, 6, 10, 9, 5, 7, 2, 4, 8, 3

51. b. Critical path: 1, 2, 5, 8, 9

SECTION 9.1

2. 3/4, 1/2, 1/2

3. {1♦, 2♦, 3♦, 4♦, 5♦, 6♦, 7♦, 8♦, 9♦, 10♦, 1♥, 2♥, 3♥, 4♥, 5♥, 6♥, 7♥, 8♥, 9♥, 10♥}, probability = $20/52 \cong 38.5\%$

5. {10♣, J♣, Q♣, K♣, A♣, 10♦, J♦, Q♦, K♦, A♦, 10♥, J♥, Q♥, K♥, A♥, 10♠, J♠, Q♠, K♠, A♠}, probability = $20/52 = 5/13 \cong 38.5\%$

7. {26, 35, 44, 53, 62}, probability = $3/8 \cong 37.5\%$

9. {11, 12, 13, 14, 15, 21, 22, 23, 24, 31, 32, 33, 41, 42, 51}, probability = $15/36 = 41\frac{2}{3}\%$

11. a. {*HHH*, *HHT*, *HTH*, *HTT*, *THH*, *THT*, *TTH*, *TTT*}

b. (i) {*HTT*, *THT*, *TTH*}, probability = $3/8 \cong 37.5\%$

12. a. {*BBB*, *BBG*, *BGB*, *BGG*, *GBB*, *GBG*, *GGB*, *GGG*}

b. (i) {*GBB*, *BGB*, *BBG*}, probability = $3/8 = 37.5\%$

13. a. {*CCC*, *CCW*, *CWC*, *CWW*, *WCC*, *WCW*, *WWC*, *WWW*}

b. (i) {*CWW*, *WCW*, *WWC*}, probability = $3/8 = 37.5\%$

14. a. probability = $3/8 = 37.5\%$

16. a. {*RRR*, *RRB*, *RRY*, *RBR*, *RBB*, *RBY*, *RYR*, *RYB*, *RYY*, *BRR*, *BRB*, *BRY*, *BBR*, *BBB*, *BBY*, *BYR*, *BYB*, *BYY*, *YRR*, *YRB*, *YRY*, *YBR*, *YBB*, *YBY*, *YYR*, *YYB*, *YYY*}

b. {*RBY*, *RYB*, *YBR*, *BRY*, *BYR*, *YRB*}, probability = $6/27 = 2/9 \cong 22.2\%$

c. {*RRB*, *RBR*, *BRR*, *RRY*, *RYR*, *YRR*, *BBR*, *BRB*, *RBB*, *BBY*, *BYB*, *YBB*, *YYR*, *YRY*, *RYY*, *YYB*, *YBY*, *BYY*}, probability = $18/27 = 2/3 = 66\frac{2}{3}\%$

18. a. {B_1B_1, B_1B_2, B_1W, B_2B_1, B_2B_2, B_2W, WB_1, WB_2, WW}

b. {B_1B_1, B_1B_2, B_2B_1, B_2B_2}, probability = $4/9 \cong 44.4\%$

c. {B_1W, B_2W, WB_1, WB_2}, probability = $4/9 \cong 44.4\%$

21. a.

10	11	12	13	14	15	16	17	18	…	96	97	98	99
		↕		↕		↕		↕		↕			↕
		3·4		3·5		3·6		3·32		3·33			

The above diagram shows that there are as many positive two-digit integers that are multiples of 3 as there are integers from 4 to 33 inclusive. By Theorem 9.1.1, there are $33 - 4 + 1$, or 30, such integers.

b. There are $99 - 10 + 1 = 90$ positive two-digit integers in all, and by part (a), 30 of these are multiples of 3. So the probability that a randomly chosen positive two-digit integer is a multiple of 3 is $30/90 = 1/3 = 33\frac{1}{3}\%$.

c. Of the integers from 10 through 99 that are multiples of 4, the smallest is 12 ($=4\cdot 3$) and the largest is 96 ($=4\cdot 24$). Thus there are $24 - 3 + 1 = 22$ two-digit integers that are multiples of 4. Hence the probability that a randomly chosen two-digit integer is a multiple of 4 is $22/90 = 36\frac{2}{3}\%$.

23. c. Probability $= \frac{m-3+1}{n} = \frac{m-2}{n}$

d. Because $\left\lfloor \frac{39}{2} \right\rfloor = 19$, the probability is $\frac{39-19+1}{39} = \frac{21}{39}$.

24. a. (i) If n is even, there are $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ elements in the sub-array.

(ii) If n is odd, there are $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ elements in the sub-array.

b. There are n elements in the array, so

(i) The probability that an element is in the given sub-array when n is even is $\frac{\frac{n}{2}}{n} = \frac{1}{2}$,

(ii) The probability that an element is in the given sub-array when n is odd is $\frac{\frac{n-1}{2}}{n} = \frac{n-1}{2n}$.

26. Let k be the 27th element in the array. By Theorem 9.1.1, $k - 42 + 1 = 27$, and so $k = 42 + 27 - 1 = 68$. Thus the 27th element in the array is $A[68]$.

28. Let m be the smallest of the integers. By Theorem 9.1.1, $279 - m + 1 = 56$, and so $m = 279 - 56 + 1 = 224$. Thus the smallest of the integers is 224.

31.

1	2	3	4	5	6	7	8	9	…	999	1000	1001
		↕			↕			↕		↕		
		$3\cdot 1$			$3\cdot 2$			$3\cdot 3$		$3\cdot 333$		

Thus there are 333 multiples of 3 between 1 and 1001.

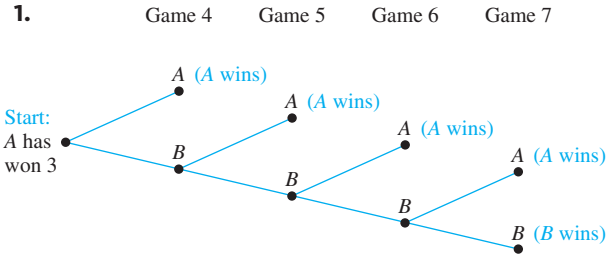
32. a.

M	Tu	W	Th	F	Sa	Su	M	Tu	W	Th	F	Sa	Su	…	F	Sa	Su	M
1	2	3	4	5	6	7	8	9	10	11	12	13	14		362	363	364	365
						↕							↕				↕	
						$7\cdot 1$							$7\cdot 2$				$7\cdot 52$	

Sundays occur on the 7th day of the year, the 14th day of the year, and in fact on all days that are multiples of 7. There are 52 multiples of 7 between 1 and 365, and so there are 52 Sundays in the year.

SECTION 9.2

1.

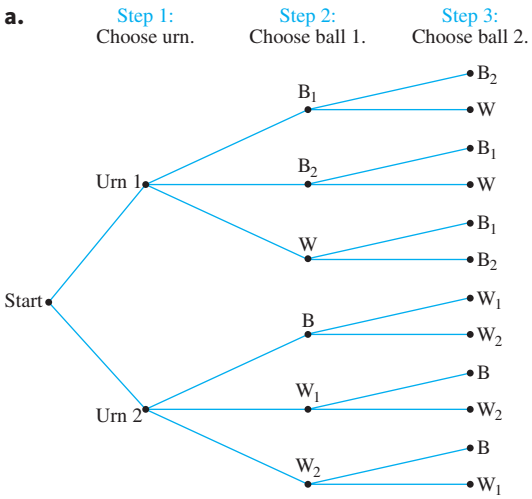


There are five ways to complete the series: A, B–A, B–B–A, B–B–B–A, and B–B–B–B.

3. Four ways: A–A–A–A, B–A–A–A–A, B–B–A–A–A–A, and B–B–B–A–A–A–A

4. Two ways: A–B–A–B–A–B–A and B–A–B–A–B–A–B

6. a.



b. There are 12 equally likely outcomes of the experiment.

c. $2/12 = 1/6 = 16\frac{2}{3}\%$ **d.** $8/12 = 2/3 = 66\frac{2}{3}\%$

8. By the multiplication rule, the answer is $3\cdot 2\cdot 2 = 12$.

9. a. In going from city A to city B, one may take any of the 3 roads. In going from city B to city C, one may take any of the 5 roads. So, by the multiplication rule, there are $3\cdot 5 = 15$ ways to travel from city A to city C via city B.

b. A round-trip journey can be thought of as a four-step operation:

Step 1: Go from A to B.

Step 2: Go from B to C.

Step 3: Go from C to B.

Step 4: Go from B to A.

Since there are 3 ways to perform step 1, 5 ways to perform step 2, 5 ways to perform step 3, and

3 ways to perform step 4, by the multiplication rule, there are $3 \cdot 5 \cdot 5 \cdot 3 = 225$ round-trip routes.

c. In this case the steps for making a round-trip journey are the same as in part (b), but since no route segment may be repeated, there are only 4 ways to perform step 3 and only 2 ways to perform step 4. So, by the multiplication rule, there are $3 \cdot 5 \cdot 4 \cdot 2 = 120$ round-trip routes in which no road is traversed twice.

11. a. Imagine constructing a bit string of length 8 as an eight-step process:

Step 1: Choose either a 0 or a 1 for the left-most position,

Step 2: Choose either a 0 or a 1 for the next position to the right.

⋮

Step 8: Choose either a 0 or a 1 for the right-most position.

Since there are 2 ways to perform each step, the total number of ways to accomplish the entire operation, which is the number of different bit strings of length 8, is $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8 = 256$.

b. Imagine that there are three 0's in the three left-most positions, and imagine filling in the remaining 5 positions as a five-step process, where step i is to fill in the $(i+3)$rd position. Since there are 2 ways to perform each of the 5 steps, there are 2^5 ways to perform the entire operation. So there are 2^5, or 32, 8-bit strings that begin with three 0's.

12. a. Think of creating a hexadecimal number that satisfies the given requirements as a five-step process.

Step 1: Choose the left-most hexadecimal digits. It can be any of the 9 hexadecimal digits from 3 through B.

Steps 2–4: Choose the three hexadecimal digits for the middle three positions. Each can be any of the 16 hexadecimal digits.

Step 5: Choose the right-most hexadecimal digit. It can be any of the 11 hexadecimal digits from 5 through F.

There are 9 ways to perform step 1, 16 ways to perform each of steps 2 through 4, and 11 ways to perform step 5. Thus, the total number of specified hexadecimal numbers is $9 \cdot 16 \cdot 16 \cdot 16 \cdot 11 = 405{,}504$.

13. a. In each of the four tosses there are two possible results: Either a head (H) or a tail (T) is obtained. Thus, by the multiplication rule, the number of outcomes is $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$.

b. There are six outcomes with two heads: *HHTT*, *HTHT*, *HTTH*, *THHT*, *THTH*, *TTHH*. Thus the probability of obtaining exactly two heads is $6/16 = 3/8$.

14. a. Think of creating license plates that satisfy the given conditions as the following seven-step process: In steps 1–4 choose the letters to put in positions 1–4, and in steps 5–7, choose the digits to put in positions 5–7. Since there are 26 letters and 10 digits and since repetition is allowed, there are 26 ways to perform each of steps 1–4 and 10 ways to perform each of steps 5–7. Thus the number of license plates is

$$26 \cdot 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 456{,}976{,}000.$$

b. In this case there is only one way to perform step 1 (because the first letter must be an A) and only one way to perform step 7 (because the last digit must be a 0). Therefore, the number of license plates is $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 = 1{,}757{,}600$.

d. In this case there are 26 ways to perform step 1, 25 ways to perform step 2, 24 ways to perform step 5, and 8 ways to perform step 6, so the number of license plates is $26 \cdot 25 \cdot 24 \cdot 23 \cdot 10 \cdot 9 \cdot 8 = 258{,}336{,}000$.

16. a. Two solutions:

(i) By the multiplication rule, the number of integers from 10 through 99

$$= \begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the first digit}\end{bmatrix}\begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the second digit}\end{bmatrix}$$

$$= 9 \cdot 10 = 90$$

(ii) By Theorem 9.1.1, the number of integers from 10 through $99 = 90 - 10 + 1 = 90$.

b. Because odd integers end in 1, 3, 5, 7, or 9, the number of odd integers from 10 through 99

$$= \begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the first digit}\end{bmatrix}\begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the second digit}\end{bmatrix}$$

$$= 9 \cdot 5 = 45.$$

An alternative solution uses the listing method shown in the solution for Example 9.1.4.

c. $\begin{bmatrix}\text{the number of integers}\\ \text{with distinct digits}\end{bmatrix}$

$$= \begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the first digit}\end{bmatrix}\begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the second digit}\end{bmatrix}$$

$$= 9 \cdot 9 = 81$$

d. $\begin{bmatrix}\text{the number of odd integers}\\ \text{with distinct digits}\end{bmatrix}$

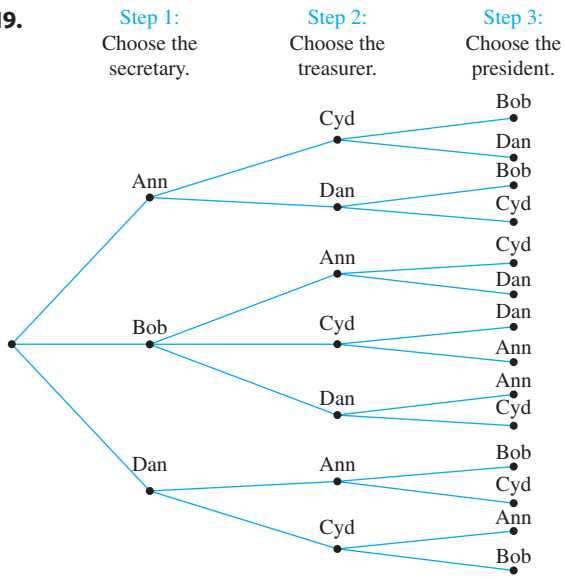
$$= \begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the second digit}\end{bmatrix}\begin{bmatrix}\text{the number of}\\ \text{ways to pick}\\ \text{the first digit}\end{bmatrix}$$

$= 5 \cdot 8 = 40$ because the first digit can't equal 0, nor can it equal the second digit

e. $81/90 = 9/10$, $40/90 = 4/9$

18. a. Let step 1 be to choose either the number 2 or one of the letters corresponding to the number 2 on the keypad, let step 2 be to choose either the number 1 or one of the letters corresponding to the number 1 on the keypad, and let steps 3 and 4 be to choose either the number 3 or one of the letters corresponding to the number 3 on the keypad. There are 4 ways to perform step 1, 3 ways to perform step 2, and 4 ways to perform each of steps 3 and 4. So by the multiplication rule, there are $4 \cdot 3 \cdot 4 \cdot 4 = 192$ ways to perform the entire operation. Thus there are 192 different PINs that are keyed the same as 2133. Note that on a computer keyboard, these PINs would not be keyed the same way.

19.



There are 14 different paths from "root" to "leaf" of this possibility tree, and so there are 14 ways the officers can be chosen. Because $14 = 2 \cdot 7$, reordering the steps will not make it possible to use the multiplication rule alone to solve this problem.

20. a. The number of ways to perform step 4 is not constant; it depends on how the previous steps were performed. For instance, if 3 digits had been chosen in steps 1–3, then there would be $10 - 3 = 7$ ways to perform step 4, but if 3 letters had been chosen in steps 1–3, then there would be 10 ways to perform step 4.

21. *Hint:*
a. The answer is 2^{mn}. **b.** The answer is n^m.

22. a. The answer is $4 \cdot 4 \cdot 4 = 4^3 = 64$. Imagine creating a function from a 3-element set to a 4-element set as a three-step process: Step 1 is to send the first element of the 3-element set to an element of the 4-element set (there are four ways to perform this step); step 2 is to send the second element of the 3-element set to an element of the 4-element set (there are also four ways to perform this step); and step 3 is to send the third element of the 3-element set to an element of the 4-element set (there are four ways to perform this step). Thus the entire process can be performed in $4 \cdot 4 \cdot 4$ different ways.

24. The outer loop is iterated 30 times, and during each iteration of the outer loop there are 15 iterations of the inner loop. Hence, by the multiplication rule, the total number of iterations of the inner loop is $30 \cdot 15 = 450$.

27. The outer loop is iterated $50 - 5 + 1 = 46$ times, and during each iteration of the outer loop there are $20 - 10 + 1 = 11$ iterations of the inner loop. Hence, by the multiplication rule, the total number of iterations of the inner loop is $46 \cdot 11 = 506$.

29. *Hint:* An efficient solution is to add leading zeros as needed to make each number five digits long. For instance, write 1 as 00001. Then, instead of choosing digits for the positions, choose positions for the digits. The answer is 720.

31. a. There are $a + 1$ divisors: $1, p, p^2, \ldots, p^a$.
b. A divisor is a product of any one of the $a + 1$ numbers listed in part (a) times any one of the $b + 1$ numbers $1, q, q^2, \ldots, q^b$. So, by the multiplication rule, there are $(a + 1)(b + 1)$ divisors in all.

32. a. Since the nine letters of the word *ALGORITHM* are all distinct, there are as many arrangements of these letters in a row as there are permutations of a set with nine elements: $9! = 362{,}880$.
b. In this case there are effectively eight symbols to be permuted (because $\boxed{AL}$ may be regarded as a single symbol). So the number of arrangements is $8! = 40{,}320$.

34. The same reasoning as in Example 9.2.9 gives an answer of $4! = 24$.

35. *WX, WY, WZ, XW, XY, XZ, YW, YX, YZ, ZW, ZX, ZY*

37. a. $P(6, 4) = \dfrac{6!}{(6-4)!} = \dfrac{6 \cdot 5 \cdot 4 \cdot 3 \cdot \cancel{2} \cdot \cancel{1}}{\cancel{2} \cdot \cancel{1}} = 360$

38. a. $P(5, 3) = \dfrac{5 \cdot 4 \cdot 3 \cdot \cancel{2!}}{\cancel{2!}} = 60$

39. a. $P(9, 3) = \dfrac{9 \cdot 8 \cdot 7 \cdot \cancel{6!}}{\cancel{6!}} = 504$

c. $P(8, 5) = \dfrac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot \cancel{3!}}{\cancel{3!}} = 6{,}720$

41. Proof: Let n be an integer and $n \geq 2$. Then

$$P(n+1, 2) - P(n, 2)$$

$$= \frac{(n+1)!}{[(n+1)-2]!} - \frac{n!}{(n-2)!} = \frac{(n+1)!}{(n-1)!} - \frac{n!}{(n-2)!}$$

$$= \frac{(n+1)\cdot n\cdot \cancel{(n-1)!}}{\cancel{(n-1)!}} - \frac{n\cdot(n-1)\cdot \cancel{(n-2)!}}{\cancel{(n-2)!}}$$

$$= n^2 + n - (n^2 - n) = 2n = 2\cdot\frac{n\cdot(n-1)!}{(n-1)!}$$

$$= 2\cdot\frac{n!}{(n-1)!} = 2P(n, 1).$$

This is what was to be proved.

45. *Hint:* Let $P(n)$ be the sentence, "There are $n!$ permutations of a set with n elements." In the inductive step, assume $P(k)$ is true, and let X be a set with $k+1$ elements. Use a 2-step operation to create a permutation of the elements of X, where step 1 is to choose the element to write first, and step 2 is to write the remaining elements of X in some order.

47. a.

1	2	3	1	2	3	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	2	1	3	3	2	1

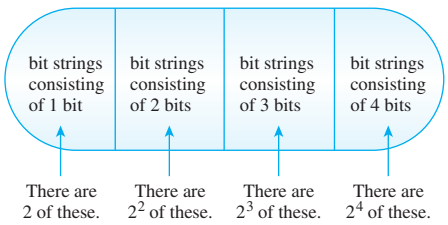
1	2	3	1	2	3	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	3	2	2	3	1	3	1	2

b.

1	2	3	1	2	3
↓	↓	↓	↓	↓	↓
2	3	1	3	1	2

SECTION 9.3

1. a. Think of creating a bit string with n bits as an n-step process where a general step k is to place either a 0 or a 1 in the kth position. Since there are two ways to do this for each position, by the multiplication rule, the number of bit strings of length k is 2^k. Now the set of all bit strings consisting of from 1 through 4 bits can be broken into four disjoint subsets:



Applying the addition rule to the figure shows that there are $2 + 2^2 + 2^3 + 2^4 = 30$ bit strings consisting of from one through four bits.

b. By reasoning similar to that of part (a), there are $2^5 + 2^6 + 2^7 + 2^8 = 480$ bit strings of from five through eight bits.

3. a. The set of integers from 1 through 999 with no repeated digit can be broken into three disjoint subsets: those from 1 through 9, those from 1 through 99, and those from 100 through 999. Now constructing an integer from 100 through 999 with no repeated digit can be thought of as a three-step process.

Step 1: Choose a digit for the left-most position (where there are 9 choices because 0 cannot be chosen).

Step 2: Choose a digit for the middle position (where there are also 9 choices because the digit in the left-most position cannot be reused but 0 can be used).

Step 3: Choose a digit for the right-most position (where there are 8 choices because neither of the other two digits can be reused).

Thus there are $9\cdot9\cdot8$ integers from 100 through 999 with no repeated digit. Similar reasoning shows that there are $9\cdot9$ integers from 10 through 99 with no repeated digit. Finally, there are clearly 9 integers from 1 through 9 with no repeated digit. Hence, by the addition rule, the number of integers from 1 through 999 with no repeated digit is $9 + 9\cdot9 + 9\cdot9\cdot8 = 738$.

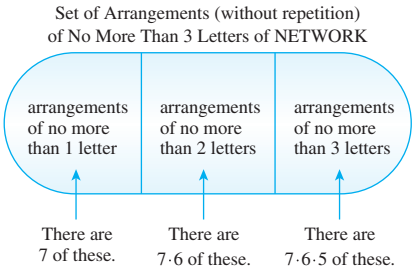
b. [number of integers from 1 through 999 with at least one repeated digit]

$$= \left[\begin{array}{l}\text{total number of}\\ \text{integers from}\\ \text{1 through 999}\end{array}\right] - \left[\begin{array}{l}\text{number of integers}\\ \text{from 1 through 999}\\ \text{with no repeated digits}\end{array}\right]$$

$$= 999 - 738 = 261$$

c. The probability that an integer chosen at random has at least one repeated digit is $261/999 \cong 26.1\%$.

4. Use the multiplication rule to count the elements in each of the three sets containing 1, 2, and 3 letters, respectively. Then, because these sets are disjoint, use the addition rule to compute the total number of elements in the three sets taken together.



Applying the addition rule to the figure above shows that there are $7 + 7\cdot6 + 7\cdot6\cdot5 = 259$ arrangements of three letters of the word *NETWORK* if repetition of letters is not permitted.

6. In this exercise the 26 letters in the alphabet plus the 10 digits give a total of 36 symbols that can be used on a license plate.

a. Imagine constructing a license plate with 4 symbols as a four-step process: step 1 is to fill in the first symbol, step 2 is to fill in the second symbol, step 3 is to fill in the third symbol, and step 4 is to fill in the fourth symbol. Because any one of the 36 symbols can be used in each step, by the multiplication rule, the number of license plates that use four symbols is 36^4. Similarly, the number that use 5 symbols is 36^5, and the number that use six symbols is 36^6. Thus because license plates can have anywhere from 4 to 6 symbols, the total number of plates with repeated symbols allowed is

$$36^4 + 36^5 + 36^6 = 2{,}238{,}928{,}128.$$

b. When repetition is not allowed, the number of license plates that use four symbols is $36 \cdot 35 \cdot 34 \cdot 33$. The reason is that in the second step the symbol used in the first step cannot be used, so there are only 35 choices for the second step. In the third step, neither of the symbols used in the first two steps can be used, and so there are only 34 choices for the third step. And in the fourth step, none of the symbols used in the first three steps can be used, and so there are only 33 choices for the fourth step. Similarly, the number of license plates that use 5 symbols is $36 \cdot 35 \cdot 34 \cdot 33 \cdot 32$, and the number that use six symbols is $36 \cdot 35 \cdot 34 \cdot 33 \cdot 32 \cdot 31$. Thus the total number of license plates is

$$36 \cdot 35 \cdot 34 \cdot 33 + 36 \cdot 35 \cdot 34 \cdot 33 \cdot 32 + 36 \cdot 35 \cdot 34 \cdot 33 \cdot 32 \cdot 31 = 1{,}449{,}063{,}000.$$

c. Consider two sets: the set of plates with repetition not allowed and the set of plates that have a repeated symbol. Note that these two sets have no elements in common, and that since every license plate either has a repeated symbol or does not have a repeated symbol, every license plate considered in part (a) is in one of the two sets. In other words, the set of all license plates with repetition allowed is composed of two disjoint subsets: the set of plates with repetition not allowed and the set of plates that have a repeated symbol. Thus, by the difference rule, the number of license plates with a repeated symbol is the difference between the number of plates with repetition allowed minus the number of plates with repetition not allowed:

$$2{,}238{,}928{,}128 - 1{,}449{,}063{,}000 = 789{,}865{,}128.$$

d. The probability that a license plate chosen at random has at least one repeated symbol is $\frac{789{,}865{,}128}{2{,}238{,}928{,}128} \cong 35.3\%$.

7. **a.** The 26 letters in the alphabet plus the 10 digits plus the 14 special characters give a total of 50 symbols that can be used. By the multiplication rule, the number of passwords with 3, 4, and 5 symbols is 50^3, 50^4, and 50^5. Since the sets consisting of these passwords are disjoint, by the addition rule, the number of passwords is

$$50^3 + 50^4 + 50^5 = 318{,}875{,}000.$$

8. **a.** *Hint:* One approach is to divide the license plates into four groups depending on the number of digits and letters they contain. Another approach is to consider creating a license plate as a two-step process: *step 1*: either choose one digit or do not choose a digit; and *step 2*: choose 4 or 5 letters.

9. **a.** Each column of the table below corresponds to a pair of values of i and j for which the inner loop will be iterated.

i	1	2 →		3 →			4 →			
j	1	1	2	1	2	3	1	2	3	4
		1		2			3			4

Since there are $1 + 2 + 3 + 4 = 10$ columns, the inner loop will be iterated ten times.

11. **a.** The answer is the number of permutations of the five letters in *QUICK*, which equals $5! = 120$.

b. Because *QU* (in order) is to be considered as a single unit, the answer is the number of permutations of the four symbols $\boxed{QU}$, *I*, *C*, *K*. This is $4! = 24$.

c. By part (b), there are 4! arrangements of $\boxed{QU}$, *I*, *C*, *K*. Similarly, there are 4! arrangements of $\boxed{UQ}$, *I*, *C*, *K*. Therefore, by the addition rule, there are $4! + 4! = 48$ arrangements in all.

13. **a.**

$$\left[\begin{array}{l}\text{the number of ways to place eight people}\\ \text{in a row keeping } A \text{ and } B \text{ together}\end{array}\right]$$

$$= \left[\begin{array}{l}\text{the number of ways to arrange}\\ \boxed{AB}\ C\ D\ E\ F\ G\ H\end{array}\right] + \left[\begin{array}{l}\text{the number of ways to arrange}\\ \boxed{BA}\ C\ D\ E\ F\ G\ H\end{array}\right]$$

$$= 7! + 7! = 5{,}040 + 5{,}040 = 10{,}080$$

b.

$$\left[\begin{array}{l}\text{the number of ways to arrange the eight}\\ \text{people in a row keeping } A \text{ and } B \text{ apart}\end{array}\right]$$

$$= \left[\begin{array}{l}\text{the total number of ways}\\ \text{to place the eight}\\ \text{people in a row}\end{array}\right] - \left[\begin{array}{l}\text{the number of ways to place}\\ \text{the eight people in a row}\\ \text{keeping } A \text{ and } B \text{ together}\end{array}\right]$$

$$= 8! - 10{,}080 = 40{,}320 - 10{,}080$$

$$= 30{,}240$$

14. the number of variable names

$$= \begin{bmatrix}\text{the number of numeric}\\ \text{variable names}\end{bmatrix} + \begin{bmatrix}\text{the number of string}\\ \text{variable names}\end{bmatrix}$$

$$= (26 + 26\cdot 36) + (26 + 26\cdot 36) = 1{,}924$$

15. *Hint:* In exercise 14 note that

$$26 + 26\cdot 36 = 26\sum_{k=0}^{1} 36^k.$$

Generalize this idea here. Use Theorem 5.2.3 to evaluate the expression you obtain.

16. a. $10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4 = 604{,}800$

b. $\begin{bmatrix}\text{the number of phone numbers}\\ \text{with at least one repeated digit}\end{bmatrix}$

$$= \begin{bmatrix}\text{the total number}\\ \text{of phone numbers}\end{bmatrix} - \begin{bmatrix}\text{the number of phone numbers}\\ \text{with no repeated digits}\end{bmatrix}$$

$$= 10^7 - 604{,}800 = 9{,}395{,}200$$

c. $\dfrac{9{,}395{,}200}{10^7} \cong 93.95\%$

18. a. Proof: Let A and B be mutually disjoint events in a sample space S. By the addition rule, $N(A \cup B) = N(A) + N(B)$. Therefore, by the equally likely probability formula,

$$P(A \cup B) = \frac{N(A \cup B)}{N(S)} = \frac{N(A) + N(B)}{N(S)}$$

$$= \frac{N(A)}{N(S)} + \frac{N(B)}{N(S)} = P(A) + P(B).$$

19. *Hint:* Justify the following answer: $39\cdot 38\cdot 38$.

20. a. Use strings of five digits to represent integers from 1 to 100,000 that contain the digit 6 exactly once. For example, use 00306 to represent 306. Strings of six digits are not needed because 100,000 does not contain a 6. Imagine constructing a five-digit string that contains exactly one 6 as a five-step operation to fill in five positions with five digits: $\underline{\ }_1\ \underline{\ }_2\ \underline{\ }_3\ \underline{\ }_4\ \underline{\ }_5$.

Step 1: Choose one of the five positions for the 6.

Step 2: Choose a digit for the left-most remaining position.

Step 3: Choose a digit for the next remaining position to the right.

Step 4: Choose a digit for the next remaining position to the right.

Step 5: Choose a digit for the right-most position.

Since there are 5 choices for step 1 (any one of the five positions) and 9 choices for each of steps 2–5 (any digit except 6), by the multiplication rule, the number of ways to perform this operation is $5\cdot 9\cdot 9\cdot 9\cdot 9 = 32{,}805$. Hence there are 32,805 integers from 1 to 100,000 that contain the digit 6 exactly once.

21. *Hint:* The answer is $2/3$.

23. a. Let A = the set of integers that are multiples of 4 and B = the set of integers that are multiples of 7. Then $A \cap B$ = the set of integers that are multiples of 28.

Now $N(A) = 250$ since 1 2 3 4 5 6 7 8 . . . 999 1000,
↕ ↕ ↕
$4\cdot 1$ $4\cdot 2$ . . . $4\cdot 250$
or, equivalently, since $1{,}000 = 4\cdot 250$.

Also $N(B) = 142$ since 1 2 3 4 5 6 7 . . . 14 . . . 994 995 . . . 1000
↕ ↕ ↕
$7\cdot 1$ $7\cdot 2$ . . . $7\cdot 142$
or, equivalently, since $1{,}000 = 7\cdot 142 + 6$.

And $N(A \cap B) = 35$ since 1 2 3 . . . 28 . . . 56 . . . 980 . . . 1000,
↕ ↕ ↕
$28\cdot 1$ $28\cdot 2$ . . . $28\cdot 35$
or, equivalently, since $1{,}000 = 28\cdot 35 + 20$.

So $N(A \cup B) = 250 + 142 - 35 = 357$.

25. a. Length 0 : λ

Length 1: 0, 1

Length 2: 00, 01, 10, 11

Length 3: 000, 001, 010, 011, 100, 101, 110

Length 4: 0000, 0001, 0010, 0011, 0100, 0101, 0110, 1000, 1001, 1010, 1011, 1100, 1101

b. By part (a), $d_0 = 1$, $d_1 = 2$, $d_2 = 4$, $d_3 = 7$, and $d_4 = 13$.

c. Let k be an integer with $k \geq 3$. Any string of length k that does not contain the bit pattern 111 starts either with a 0 or with a 1. If it starts with a 0, this can be followed by any string of $k-1$ bits that does not contain the pattern 111. There are d_{k-1} of these. If the string starts with a 1, then the first two bits are 10 or 11. If the first two bits are 10, then these can be followed by any string of $k-2$ bits that does not contain the pattern 111. There are d_{k-2} of these. If the string starts with a 11, then the third bit must be 0 (because the string does not contain 111), and these three bits can be followed by any string of $k-3$ bits that does not contain the pattern 111. There are d_{k-3} of these. Therefore, for every integer $k \geq 3$, $d_k = d_{k-1} + d_{k-3}$.

d. By parts (b) and (c), $d_5 = d_4 + d_3 + d_2 = 13 + 7 + 4 = 24$. This is the number of bit strings of length five that do not contain the pattern 111.

26. c. *Hint:* $s_k = 2s_{k-1} + 2s_{k-2}$

e. *Hint:* For every integer $n \geq 0$,

$$s_n = \frac{\sqrt{3}+2}{2\sqrt{3}}(1+\sqrt{3})^n + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^n.$$

28. a. $a_3 = 3$ (The three permutations that do not move more than one place from their "natural" positions are 213, 132, and 123.)

29. a. $11001010_2 = 2 + 2^3 + 2^6 + 2^7 = 202$

$00111000_2 = 2^3 + 2^4 + 2^5 = 56$

$01101011_2 = 1 + 2 + 2^3 + 2^5 + 2^6 = 107$

$11101110_2 = 2 + 2^2 + 2^3 + 2^5 + 2^6 + 2^7 = 238$

So the answer is 202.56.107.238.

b. The network ID for a Class *A* network consists of 8 bits and begins with 0. If all possible combinations of eight 0's and l's that start with a 0 were allowed, there would be 2 choices (0 or 1) for each of the 7 positions from the second through the eighth. This would give $2^7 = 128$ possible ID's. But because neither 00000000 nor 01111111 is allowed, the total is reduced by 2, so there are 126 possible Class *A* networks.

c. Let *w.x.y.z* be the dotted decimal form of the IP address for a computer in a Class *A* network. Because the network IDs for a Class *A* network go from 00000001 (=1) through 01111110 (=126), *w* can be any integer from 1 through 126. In addition, each of *x*, *y*, and *z* can be any integer from 0 (=00000000) through 255 (=11111111), except that *x*, *y*, and *z* cannot all be 0 simultaneously and cannot all be 255 simultaneously.

d. Twenty-four positions are allocated for the host ID in a Class *A* network. If each could be either 0 or 1, there would be $2^{24} = 16{,}777{,}216$ possible host IDs. But neither all 0's nor all 1's is allowed, which reduces the total by 2. Thus there are 16,777,214 possible host IDs in a Class *A* network.

i. Observe that $140 = 128 + 8 + 4 = 10001100_2$, which begins with 10. Thus the IP address comes from a Class *B* network. An alternative solution uses the result of Example 9.3.5: Network IDs for Class *B* networks range from 128 through 191. Thus, since $128 \leq 140 \leq 191$, the given IP address is from a Class *B* network.

31. a. There are 12 possible birth months for *A*, 12 for *B*, 12 for *C*, and 12 for *D*, so the total is $12^4 = 20{,}736$.

b. If no two people share the same birth month, there are 12 possible birth months for *A*, 11 for *B*, 10 for C, and 9 for *D*. Thus the total is $12 \cdot 11 \cdot 10 \cdot 9 = 11{,}880$.

c. If at least two people share the same birth month, the total number of ways birth months could be associated with *A*, *B*, *C*, and *D* is $20{,}736 - 11{,}880 = 8{,}856$.

d. The probability that at least two of the four people share the same birth month is $\frac{8{,}856}{20{,}736} \cong 42.7\%$.

e. When there are five people, the probability that at least two share the same birth month is $\frac{12^5 - 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{12^5} \cong 61.8\%$, and when there are more than five people, the probability is even greater. Thus, since the probability for four people is less than 50%, the group must contain five or more people for the probability to be at least 50% that two or more share the same birth month.

32. *Hint:* Analyze the solution to exercise 31.

33. a. The number of students who checked at least one of the statements is $N(H) + N(C) + N(D) - N(H \cap C) - N(H \cap D) - N(C \cap D) + N(H \cap C \cap D) = 28 + 26 + 14 - 8 - 4 - 3 + 2 = 55$.

b. By the difference rule, the number of students who checked none of the statements is the total number of students minus the number who checked at least one statement. This is $100 - 55 = 45$.

d. The number of students who checked #1 and #2 but not #3 is $N(H \cap D) - N(H \cap C \cap D) = 8 - 2 = 6$.

35. Let

$M =$ the set of married people in the sample,

$Y =$ the set of people between 20 and 30 in the sample, and

$F =$ the set of females in the sample.

Then the number of people in the set $M \cup Y \cup F$ is less than or equal to the size of the sample. And so

$$\begin{aligned} 1{,}200 &\geq N(M \cup Y \cup F) \\ &= N(M) + N(Y) + N(F) - N(M \cap Y) \\ &\quad - N(M \cap F) - N(Y \cap F) + N(M \cap Y \cap F) \\ &= 675 + 682 + 684 - 195 - 467 - 318 + 165 \\ &= 1{,}226. \end{aligned}$$

This is impossible since $1{,}200 < 1{,}226$, so the polltaker's figures are inconsistent. They could not have occurred as a result of an actual sample survey.

37. Let *A* be the set of all positive integers less than 1,000 that are not multiples of 2, and let *B* be the set of all positive integers less than 1,000 that are not multiples of 5. Since the only prime factors of 1,000 are 2 and 5, the number of positive integers that have no common factors with 1,000 is $N(A \cap B)$. Let the universe *U* be the set of all positive integers less than 1,000. Then A^c is the set of positive integers less than 1,000 that are multiples of 2, B^c is the set of positive integers less than 1,000 that are multiples of 5, and $A^c \cap B^c$ is the set of positive integers less than 1,000 that are multiples of 10. By one of the procedures discussed in Section 9.1 or 9.2, it is easily found that $N(A^c) = 499$, $N(B^c) = 199$,

and $N(A^c \cap B^c) = 99$. Thus, by the inclusion/exclusion rule,

$$N(A^c \cup B^c) = N(A^c) + N(B^c) - N(A^c \cap B^c)$$
$$= 499 + 199 - 99 = 599.$$

But by De Morgan's law, $N(A^c \cup B^c) = N((A \cap B)^c)$, and so

$$N((A \cap B)^c) = 599. \qquad (*)$$

Now since $(A \cap B)^c = U - (A \cap B)$, by the difference rule we have

$$N((A \cap B)^c) = N(U) - N(A \cap B). \qquad (**)$$

Equating the right-hand sides of (*) and (**) gives $N(U) - N(A \cap B) = 599$. And because $N(U) = 999$, we conclude that $999 - N(A \cap B) = 599$, or, equivalently, $N(A \cap B) = 999 - 599 = 400$. So there are 400 positive integers less than 1,000 that have no common factor with 1,000.

40. *Hint:* Let A and B be the sets of all positive integers less than or equal to n that are divisible by p and q, respectively. Then $\phi(n) = n - (N(A \cup B))$.

42. c. *Hint:* If $k \geq 6$, any sequence of k games must begin with W, LW, or LLW, where L stands for "lose" and W stands for "win."

43. c. *Hint:* Divide the set of all derangements into two subsets: one subset consists of all derangements in which the number 1 changes places with another number, and the other subset consists of all derangements in which the number 1 goes to position $i \neq 1$ but i does not go to position 1. The answer is $d_k = (k-1)d_{k-1} + (k-1)d_{k-2}$. Can you justify it?

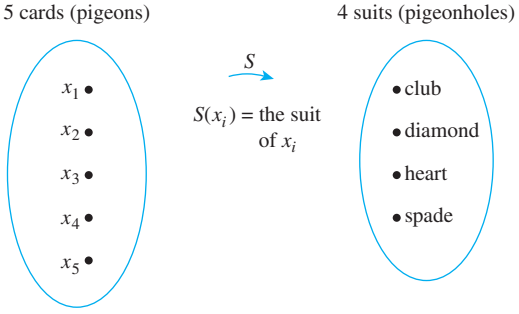
48. *Hint:* Use the associative law for sets from Theorem 6.2.2 and the generalized distributive law for sets from exercise 40, Section 6.2.

49. *Hint:* Use the solution method described in Section 5.8. The answer is $s_k = 2s_{k-1} + 3s_{k-2}$ for every integer $k \geq 4$.

SECTION 9.4

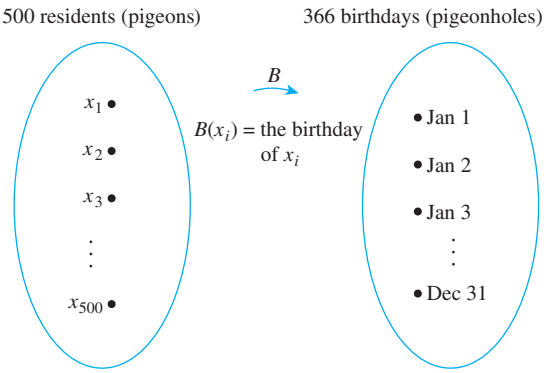
1. a. No. For instance, the aces of the four different suits could be selected.

b. Yes. Let x_1, x_2, x_3, x_4, x_5 be the five cards. Consider the function S that sends each card to its suit.



By the pigeonhole principle, S is not one-to-one: $S(x_i) = S(x_j)$ for some two cards x_i and x_j. Hence at least two cards have the same suit.

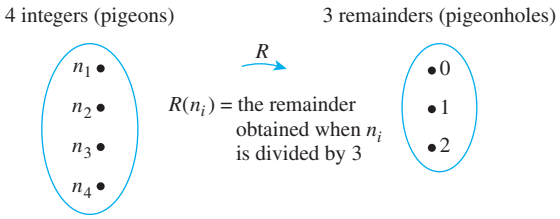
3. Yes. Denote the residents by $x_1, x_2, \ldots, x_{500}$. Consider the function B from residents to birthdays that sends each resident to his or her birthday:



By the pigeonhole principle, B is not one-to-one: $B(x_i) = B(x_j)$ for some two residents x_i and x_j. Hence at least two residents have the same birthday.

5. a. Yes. There are only three possible remainders that can be obtained when an integer is divided by 3: 0, 1, and 2. Thus, by the pigeonhole principle, if four integers are each divided by 3, then at least two of them must have the same remainder.

More formally, call the integers n_1, n_2, n_3, and n_4, and consider the function R that sends each integer to the remainder obtained when that integer is divided by 3:



By the pigeonhole principle, R is not one-to-one: $R(n_i) = R(n_j)$ for some two integers n_i and n_j. Hence at least two integers must have the same remainder.

b. No. For instance, $\{0, 1, 2\}$ is a set of three integers no two of which have the same remainder when divided by 3.

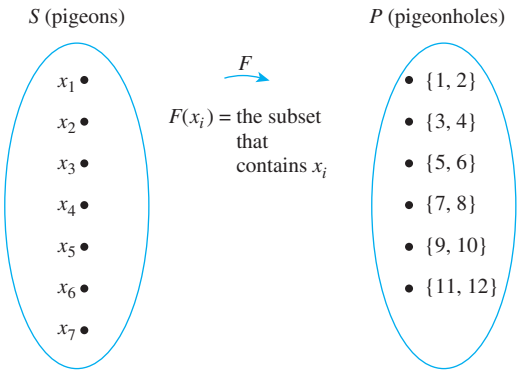
7. *Hint:* Look at Example 9.4.3.

9. a. Yes.

Solution 1: Only six of the numbers from 1 to 12 are even (namely, 2, 4, 6, 8, 10, 12), so at most six even numbers can be chosen from between 1 and 12 inclusive. Hence if seven numbers are chosen, at least one must be odd.

Solution 2: Partition the set of all integers from 1 through 12 into six subsets (the pigeonholes), each consisting of an odd and an even number: {1, 2}, {3, 4}, {5, 6}, {7, 8}, {9, 10}, {11, 12}. If seven integers (the pigeons) are chosen from among 1 through 12, then, by the pigeonhole principle, at least two must be from the same subset. But each subset contains one odd and one even number. Hence at least one of the seven numbers is odd.

Solution 3: (*a formal version of Solution* 2)*:* Let $S = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ be a set of seven numbers chosen from the set $T = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, and let P be the following partition of T: {1, 2}, {3, 4}, {5, 6}, {7, 8}, {9, 10}, and {11, 12}. Since each element of S lies in exactly one subset of the partition, we can define a function F from 5 to P by letting $F(x_i)$ be the subset that contains x_i.



Since S has 7 elements and P has 6 elements, by the pigeonhole principle, F is not one-to-one. Thus two distinct numbers of the seven are sent to the same subset, which implies that these two numbers are the two distinct elements of the subset. Therefore, since each pair consists of one odd and one even integer, one of the seven numbers is odd.

b. No. For instance, none of the 10 numbers 1, 3, 5, 7, 9, 11, 13, 15, 17, 19 is even.

10. Yes. There are n even integers in the set $\{1, 2, 3, \ldots, 2n\}$, namely, $2(= 2\cdot\underline{1})$, $4(= 2\cdot\underline{2})$, $6(= 2\cdot\underline{3}), \ldots, 2\underline{n}(= 2\cdot n)$. So the maximum number of even integers that can be chosen is n. Thus if $n + 1$ integers are chosen, at least one of them must be odd.

12. The answer is 27. There are only 26 black cards in a standard 52-card deck, so at most 26 black cards can be chosen. Hence if 27 are taken, at least one must be red.

14. There are 61 integers from 0 through 60. Of these, 31 are even ($0 = 2\cdot\underline{0}$, $2 = 2\cdot\underline{1}$, $4 = 2\cdot\underline{2}, \ldots, 60 = 2\cdot\underline{30}$) and so 30 are odd. Hence if 32 integers are chosen, at least one must be odd, and if 31 integers are chosen, at least one must be even.

17. The answer is 8. (There are only seven possible remainders for division by 7: 0, 1, 2, 3, 4, 5, 6. Hence if 8 are chosen, at least two must be the same.)

20. a. The answer is 20,483 because the possible remainders are 0, 1, 2, . . . , 20482.

b. The length of the repeating section of the decimal representation of 5/20483 is less than or equal to 20,482. The reason is that 20,482 is the number of nonzero remainders that can be obtained when a number is divided by 20,483. Thus, in the long-division process of dividing 5 by 20,483, either some remainder is 0 and the decimal expansion terminates, or only nonzero remainders are obtained and at some point within the first 20,482 successive divisions, a nonzero remainder is repeated. At that point the digits in the developing decimal expansion begin to repeat because the sequence of successive remainders repeats those previously obtained.

22. This number is irrational because the decimal expansion neither terminates nor repeats.

24. Let A be the set of the thirteen chosen numbers, and let B be the set of all prime numbers between 1 and 40. Note that $B = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$. For each x in A, let $F(x)$ be the smallest prime number that divides x. Since A has 13 elements and B has 12 elements, by the pigeonhole principle F is not one-to-one. Thus $F(x_1) = F(x_2)$ for some $x_1 \neq x_2$ in A. By definition of F, this means that the smallest prime number that divides x_1 equals the smallest prime number that divides x_2. Therefore, two numbers in A—namely, x_1 and x_2—have a common divisor greater than 1. *[Strictly speaking, only integers less than or equal to 20 can divide integers less than or equal to 40. So we could have made the set B even smaller.]*

25. Yes. This follows from the generalized pigeonhole principle with 30 pigeons, 12 pigeonholes, and $k = 2$, using the fact that $30 > 2\cdot 12$.

26. No. For instance, the birthdays of the 30 people could be distributed as follows: three birthdays in each of the six months January through June and two birthdays in each of the six months July through December.

29. The answer is $x = 3$. There are 18 years from 17 through 34. Now $40 > 18\cdot 2$, so by the generalized pigeonhole principle, you can be sure that there are at least $x = 3$ students of the same age. However, since $18\cdot 3 > 40$, you cannot be sure of having more than three students with the same age. (For instance, three students could be each of the ages 17 through 20, and two could be each of the ages from 21 through 34.) So x cannot be taken to be greater than 3.

31. *Hint:* Use the same type of reasoning as in Example 9.4.6.

32. *Hints:* (1) The number of subsets of the six integers is $2^6 = 64$. (2) Since each integer is less than 13, the largest possible sum is 57. (Why? How is this sum obtained?)

33. *Hint:* The power set of A has $2^6 = 64$ elements, and so there are 63 nonempty subsets of A. Let k be the smallest number in A. Then the sums over the elements in the nonempty subsets of A lie in the range from k through $k + 10 + 11 + 12 + 13 + 14 = k + 60$. How many numbers are in this range?

35. *Hint:* Let X be the set consisting of the given 52 positive integers, and let Y be the set containing the following elements: {00}, {50}, {01, 99}, {02, 98}, {03, 97}, . . . , {48, 52}, {49, 51}. Define a function F from X to Y by the rule $F(x) =$ the set containing the last two digits of x. Use the pigeonhole principle to argue that F is not one-to-one, and show how the desired conclusion follows.

36. *Hint:* Write the 101 integers as $x_1, x_2, x_3, \ldots, x_{101}$, and represent each x_i as $a_i \cdot 2^{k_i}$ where a_i is odd and $k_i > 0$. Now $1 < x_i \leq 200$, and so $1 \leq a_i \leq 199$ for every i. Use the fact that there are only 100 odd integers from 1 to 199 inclusive.

37. b. *Hint:* For each $k = 1, 2, \ldots, n$, let $a_k = x_1 + x_2 + \cdots + x_k$. If some a_k is divisible by n, then the problem is solved: the consecutive subsequence is $x_1, x_2, \ldots, x_k$. If no a_k is divisible by n, then $a_1, a_2, a_3, \ldots, a_n$ satisfies the hypothesis of part (a). Hence $a_j - a_i$ is divisible by n for some integers i and j with $j > i$. Write $a_j - a_i$ in terms of the x_i's to derive the given conclusion.

38. *Hint:* Let $a_1, a_2, \ldots, a_{n^2+1}$ be any sequence of $n^2 + 1$ distinct real numbers, and suppose that this sequence contains neither a strictly increasing subsequence of length $n + 1$ nor a strictly decreasing subsequence of length $n + 1$. Let S be the set of all ordered pairs of integers (i, d), where $1 \leq i \leq n$ and $1 \leq d \leq n$. For each term a_k in the sequence, let $F(a_k) = (i_k, d_k)$, where i_k is the length of the longest increasing sequence starting at a_k, and d_k is the length of the longest decreasing sequence starting at a_k. Suppose that F is one-to-one and derive a contradiction.

SECTION 9.5

1. a. 2-combinations: $\{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}$.

Hence, $\binom{3}{2} = 3$.

b. Unordered selections: $\{a, b, c, d\}, \{a, b, c, e\}, \{a, b, d, e\}, \{a, c, d, e\}, \{b, c, d, e\}$.

Hence, $\binom{5}{4} = 5$.

3. $P(7, 2) = \binom{7}{2} \cdot 2!$

5. a. $\binom{6}{0} = \dfrac{6!}{0!(6-0)!} = \dfrac{6!}{1 \cdot 6!} = 1$

b. $\binom{6}{1} = \dfrac{6!}{0!(6-1)!} = \dfrac{6 \cdot 5!}{1 \cdot 5!} = 6$

6. a. the number of committees of 6

$$= \binom{15}{6} = \frac{15!}{(15-6)!6!}$$

$$= \frac{15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9!}{9! \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = 5{,}005$$

b. [the number of committees that don't contain A and B together]

$$= \begin{bmatrix}\text{the number of committees with } A \\ \text{and five others—} \\ \text{none of them } B\end{bmatrix} + \begin{bmatrix}\text{the number of committees with } B \\ \text{and five others—} \\ \text{none of them } A\end{bmatrix} + \begin{bmatrix}\text{the number of} \\ \text{committees with} \\ \text{neither } A \text{ nor } B\end{bmatrix}$$

$$= \binom{13}{5} + \binom{13}{5} + \binom{13}{6}$$

$$= 1{,}287 + 1{,}287 + 1{,}716 = 4{,}290$$

Alternative solution:

$$\begin{bmatrix}\text{the number of committees} \\ \text{that don't contain} \\ A \text{ and } B \text{ together}\end{bmatrix}$$

$$= \begin{bmatrix}\text{the total number} \\ \text{of committees}\end{bmatrix} - \begin{bmatrix}\text{the number of committees} \\ \text{that contain both } A \text{ and } B\end{bmatrix}$$

$$= \binom{15}{6} - \binom{13}{4}$$

$$= 5{,}005 - 715 = 4{,}290$$

c. $\begin{bmatrix}\text{the number of}\\ \text{committees with}\\ \text{both } A \text{ and } B\end{bmatrix} + \begin{bmatrix}\text{the number of}\\ \text{committees with}\\ \text{neither } A \text{ nor } B\end{bmatrix}$

$$= \binom{13}{4} + \binom{13}{6} = 715 + 1{,}716 = 2{,}431$$

d. (i)

$$\begin{bmatrix}\text{the number of subsets}\\ \text{of three men}\\ \text{chosen from eight}\end{bmatrix} \cdot \begin{bmatrix}\text{the number of subsets}\\ \text{of three women}\\ \text{chosen from seven}\end{bmatrix}$$

$$= \binom{8}{3}\binom{7}{3} = 56 \cdot 35 = 1{,}960$$

(ii) $\begin{bmatrix}\text{the number of}\\ \text{committees with}\\ \text{at least one woman}\end{bmatrix}$

$$= \begin{bmatrix}\text{the total}\\ \text{number of}\\ \text{committees}\end{bmatrix} - \begin{bmatrix}\text{the number}\\ \text{of all-male}\\ \text{committees}\end{bmatrix}$$

$$= \binom{15}{6} - \binom{8}{6} = 5{,}005 - 28$$

$$= 4{,}977$$

e. $\begin{bmatrix}\text{the number of}\\ \text{ways to choose}\\ \text{two freshmen}\end{bmatrix} \cdot \begin{bmatrix}\text{the number of}\\ \text{ways to choose}\\ \text{two sophomores}\end{bmatrix}$

$$\cdot \begin{bmatrix}\text{the number of}\\ \text{ways to choose}\\ \text{two juniors}\end{bmatrix} \cdot \begin{bmatrix}\text{the number of}\\ \text{ways to choose}\\ \text{two seniors}\end{bmatrix}$$

$$= \binom{3}{2}\binom{4}{2}\binom{3}{2}\binom{5}{2}$$

$$= 540$$

8. *Hint:* The answers are **a.** 1001, **b.** (i) 420, (ii) all 1001 require proof, (iii) 175, **c.** 506, **d.** 561

9. b. $\binom{24}{3}\binom{16}{3} + \binom{24}{4}\binom{16}{2} + \binom{24}{5}\binom{16}{1} + \binom{24}{6}\binom{16}{0} = 3{,}223{,}220$

11. a. (1) 4 (because there are as many royal flushes as there are suits)

(2) $\dfrac{4}{\binom{52}{5}} = \dfrac{4}{2{,}598{,}960} \cong 0.0000015$

c. (1) $13 \cdot \binom{48}{1} = 624$ (because one can first choose the denomination of the four-of-a-kind and then choose one additional card from the 48 remaining)

(2) $\dfrac{624}{\binom{52}{5}} = \dfrac{624}{2{,}598{,}960} = 0.00024$

f. (1) Imagine constructing a straight (including a straight flush and a royal flush) as a six-step process: step 1 is to choose the lowest denomination of any card of the five (which can be any one of $A, 2, \ldots, 10$), step 2 is to choose a card of that denomination, step 3 is to choose a card of the next higher denomination, and so forth until all five cards have been selected. By the multiplication rule, the number of ways to perform this process is

$$10 \cdot \binom{4}{1}\binom{4}{1}\binom{4}{1}\binom{4}{1}\binom{4}{1} = 10 \cdot 4^5 = 10{,}240.$$

By parts (a) and (b), 40 of these numbers represent royal or straight flushes, so there are $10{,}240 - 40 = 10{,}200$ straights in all.

(2) $\dfrac{10{,}200}{\binom{52}{5}} = \dfrac{10{,}200}{2{,}598{,}960} \cong 0.0039$

13. a. $2^{10} = 1{,}024$

d. $\begin{bmatrix}\text{the number of}\\ \text{outcomes with}\\ \text{at least one head}\end{bmatrix}$

$$= \begin{bmatrix}\text{the total}\\ \text{number of}\\ \text{outcomes}\end{bmatrix} - \begin{bmatrix}\text{the number of}\\ \text{outcomes with}\\ \text{no heads}\end{bmatrix}$$

$$= 1{,}024 - 1 = 1{,}023$$

15. a. 50 **b.** 50

c. To get an even sum, both numbers must be even or both must be odd. Hence

$$\begin{bmatrix}\text{the number of subsets}\\ \text{of two integers chosen}\\ \text{from 1 through 100}\\ \text{whose sum is even}\end{bmatrix} = \begin{bmatrix}\text{the number of}\\ \text{subsets of two even}\\ \text{integers chosen from}\\ \text{the 50 even integers}\end{bmatrix} + \begin{bmatrix}\text{the number of}\\ \text{subsets of two odd}\\ \text{integers chosen from}\\ \text{the 50 odd integers}\end{bmatrix}$$

$$= \binom{50}{2} + \binom{50}{2} = 2{,}450.$$

d. To obtain an odd sum, one of the numbers must be even and the other odd. Hence the answer is $\binom{50}{1} \cdot \binom{50}{1} = 2{,}500$. Alternatively, note that the answer equals the total number of subsets of two integers

chosen from 1 through 100 minus the number of such subsets for which the sum of the elements is even. Thus the answer is $\binom{100}{2} - 2{,}450 = 2{,}500$.

17. a. Two points determine a line. Hence

$$\begin{bmatrix}\text{the number of straight}\\ \text{lines determined}\\ \text{by the ten points}\end{bmatrix} = \begin{bmatrix}\text{the number of subsets}\\ \text{of two points}\\ \text{chosen from ten}\end{bmatrix}$$

$$= \binom{10}{2} = 45.$$

19. a. $\dfrac{10!}{2!1!1!3!2!1!} = 151{,}200$ since there are 2 *A*'s, 1 *B*, 1 *H*, 3 *L*'s, 2 *O*'s, and 1 *U*

b. $\dfrac{8!}{2!1!1!2!2!} = 5{,}040$ **c.** $\dfrac{9!}{1!2!1!3!2!} = 15{,}120$

23. The rook must move seven squares to the right and seven squares up, so

$$\begin{bmatrix}\text{the number of}\\ \text{paths the rook}\\ \text{can take}\end{bmatrix} = \begin{bmatrix}\text{the number}\\ \text{of orderings}\\ \text{of seven R's}\\ \text{and seven U's}\end{bmatrix}$$ where R stands for "right" and U stands for "up"

$$= \frac{14!}{7!7!} = 3{,}432.$$

24. b. *Solution 1:* One factor can be 1, and the other factor can be the product of all the primes. (This gives 1 factorization.) One factor can be one of the primes, and the other factor can be the product of the other three. (This gives $\binom{4}{1} = 4$ factorizations.) One factor can be a product of two of the primes, and the other factor can be a product of the two other primes. The number $\binom{4}{2} = 6$ counts all possible sets of two primes chosen from the four primes, and each set of two primes corresponds to a factorization. Note, however, that the set $\{p_1, p_2\}$ corresponds to the same factorization as the set $\{p_3, p_4\}$, namely, $p_1 p_2 p_3 p_4$ (just written in a different order). In general, each choice of two primes corresponds to the same factorization as one other choice of two primes. Thus the number of factorizations in which each factor is a product of two primes is $\dfrac{\binom{4}{2}}{2} = 3$. (This gives 3 factorizations.) The foregoing cases account for all the possibilities, so the answer is $4 + 3 + 1 = 8$.

Solution 2: Let $S = \{p_1, p_2, p_3, p_4\}$. Let $p_1 p_2 p_3 p_4 = P$, and let $f_1 \cdot f_2$ be any factorization of P. The product of the numbers in any subset $A \subseteq S$ can be used for f_1, with the product of the numbers in A^c being f_2. There are as many ways to write f_1 as there are subsets of S, namely, $2^4 = 16$ (by Theorem 6.3.1). However, because $f_1 \cdot f_2 = f_2 \cdot f_1$, and because two factorizations are considered the same regardless of the order in which the factors are written, the number of ways to write P as a product of two factors is half the number of subsets of S. So the answer is $\frac{16}{2} = 8$.

25. a. There are four choices for where to send the first element of the domain (any element of the co-domain may be chosen), three choices for where to send the second (since the function is one-to-one, the second element of the domain must go to a different element of the co-domain from the one to which the first element went), and two choices for where to send the third element (again since the function is one-to-one). Thus the answer is $4 \cdot 3 \cdot 2 = 24$.

b. none

e. *Hint:* The answer is $n(n-1)\cdots(n-m+1)$.

26. a. Let the elements of the domain be called a, b, and c and the elements of the co-domain be called u and v. In order for a function from $\{a, b, c\}$ to $\{u, v\}$ to be onto, two elements of the domain must be sent to u and one to v, or two elements must be sent to v and one to u. There are as many ways to send two elements of the domain to u and one to v as there are ways to choose which elements of $\{a, b, c\}$ to send to u, namely, $\binom{3}{2} = 3$. Similarly, there are $\binom{3}{2} = 3$ ways to send two elements of the domain to v and one to u. Therefore, there are $3 + 3 = 6$ onto functions from a set with three elements to a set with two elements.

c. *Hint:* The answer is 6.

d. Consider functions from a set with four elements to a set with two elements. Denote the set of four elements by $X = \{a, b, c, d\}$ and the set of two elements by $Y = \{u, v\}$. Divide the set of all onto functions from X to Y into two categories. The first category consists of all those that send the three elements in $\{a, b, c\}$ onto $\{u, v\}$ and that send d to either u or v. The functions in this category can be defined by the following two-step process:

Step 1: Construct an onto function from $\{a, b, c\}$ to $\{u, v\}$.

Step 2: Choose whether to send d to u or to v.

By part (a), there are six ways to perform step 1, and, because there are two choices for where to send d, there are two ways to perform step 2. Thus, by the multiplication rule, there are $6 \cdot 2 = 12$ ways to define the functions in the first category.

The second category consists of all the other onto functions from X to Y: those that send all three elements in $\{a, b, c\}$ to either u or v and that send d to whichever of u or v is not the image of a, b, and c. Because there are only two choices for where to send the elements in $\{a, b, c\}$, and because d is

simply sent to wherever a, b, and c do not go, there are just two functions in the second category.

Every onto function from X to Y either sends at least two elements of X to the image of d or it does not. If it does, then it is in the first category. If it does not, then it is in the second category. Therefore, all onto functions from X to Y are in one of the two categories and no function is in both categories. So the total number of onto functions is $12 + 2 = 14$.

27. a. A relation on A is any subset of $A \times A$, and $A \times A$ has $8^2 = 64$ elements. So there are 2^{64} relations on A.

c. Form a relation that is both reflexive and symmetric by a two-step process: (1) pick a set of elements of the form (a, a) (there are eight such elements, so 2^8 sets); (2) pick a set of pairs of elements of the form (a, b) and (b, a) where $a \neq b$ (there are $(64 - 8)/2 = 28$ such pairs, so 2^{28} such sets). The answer is therefore $2^8 \times 2^{28} = 2^{36}$.

28. *Hint:* Use the difference rule and the generalization of the inclusion/exclusion rule for 4 sets. (See exercise 48 in Section 9.3.)

SECTION 9.6

1. a. $\binom{5+3-1}{5} = \binom{7}{5} = \frac{7 \cdot 6}{2} = 21$.

b. The three elements of the set are 1, 2, and 3. The 5-combinations are [1, 1, 1, 1, 1], [1, 1, 1, 1, 2], [1, 1, 1, 1, 3], [1, 1, 1, 2, 2], [1, 1, 1, 2, 3], [1, 1, 1, 3, 3], [1, 1, 2, 2, 2], [1, 1, 2, 2, 3], [1, 1, 3, 3, 3], [1, 2, 2, 2, 2], [1, 2, 2, 2, 3], [1, 2, 2, 3, 3], [1, 2, 3, 3, 3], [1, 3, 3, 3, 3], [2, 2, 2, 2, 2], [2, 2, 2, 2, 3], [2, 2, 2, 3, 3], [2, 2, 3, 3, 3], [2, 3, 3, 3, 3], and [3, 3, 3, 3, 3].

2. a. $\binom{4+3-1}{4} = \binom{6}{4} = \frac{6 \cdot 5}{2} = 15$

3. a. $\binom{20+6-1}{20} = \binom{25}{20} = 53{,}130$

b. If at least three are éclairs, then 17 additional pastries are selected from six kinds. The number of selections is $\binom{17+6-1}{17} = \binom{22}{17} = 26{,}334$.

Note: In parts (a) and (b), it is assumed that the selections being counted are unordered.

c. Let T be the set of selections of pastry that may be any one of the six kinds, let $E_{\geq 3}$ be the set of selections containing three or more éclairs, and let $E_{\geq 2}$ be the set of selections containing two or fewer éclairs. Then

$$\begin{aligned} N(E_{\leq 2}) &= N(T) - N(E_{\geq 3}) && \text{because } T = E_{\leq 2} \cup E_{\geq 3} \text{ and } E_{\leq 2} \cap E_{\geq 3} = \varnothing \\ &= 53{,}130 - 26{,}334 && \text{by parts (a) and (b)} \\ &= 26{,}796. \end{aligned}$$

Thus there are 26,796 selections of pastry containing at most two éclairs.

5. The answer equals the number of 4-combinations with repetition allowed that can be formed from a set of n elements. It is

$$\begin{aligned} \binom{4+n-1}{4} &= \binom{n+3}{4} \\ &= \frac{(n+3)(n+2)(n+1)n(\cancel{n-1)!}}{4!(\cancel{n-1)!}} \\ &= \frac{n(n+1)(n+2)(n+3)}{24}. \end{aligned}$$

8. As in Example 9.6.4, the answer is the same as the number of quadruples of integers (i, j, k, m) for which $1 \leq i \leq j \leq k \leq m \leq n$. By exercise 5, this number is $\binom{n+3}{4} = \frac{n(n+1)(n+2)(n+3)}{24}$.

10. Think of the number 20 as divided into 20 individual units and the variables x_1, x_2, and x_3 as three categories into which these units are placed. The number of units in category x_i indicates the value of x_i, in a solution of the equation. By Theorem 9.6.1, the number of ways to select 20 objects from the three categories is $\binom{20+3-1}{20} = \binom{22}{20} = \frac{22 \cdot 21}{2} = 231$, so there are 231 nonnegative integer solutions to the equation.

11. The analysis for this exercise is the same as for exercise 10 except that since each $x_i \geq 1$, we can imagine taking 3 of the 20 units, placing one in each category x_1, x_2, and x_3, and then distributing the remaining 17 units among the three categories. The number of ways to do this is $\binom{17+3-1}{17} = \binom{19}{17} = \frac{19 \cdot 18}{2} = 171$, so there are 171 positive integer solutions to the equation.

16. a. Let $L_{\geq 7}$ be the set of selections that include at least seven cans of lemonade. In this case an additional eight cans can be selected from the five types of soft drinks, and so

$$N(L_{\geq 7}) = \binom{8+5-1}{8} = \binom{12}{8} = 495.$$

Let T be the set of selections of cans in which the soft drink may be any one of the five types assuming that there are at least 15 cans of each type assuming that there are at least 15 cans of each type and let $L_{\leq 6}$ be the set of selections that contain at most six cans of lemonade. Then

$$\begin{aligned} N(L_{\leq 6}) &= N(T) - N(L_{\geq 7}) && \text{because } T = L_{\leq 6} \cup L_{\geq 7} \text{ and } L_{\leq 6} \cap L_{\geq 7} = \varnothing \\ &= 3{,}876 - 495 && \text{by the above and part (a) of Example 9.6.2} \\ &= 3{,}381. \end{aligned}$$

Thus there are 3,381 selections of fifteen cans of soft drinks that contain at most six cans of lemonade.

b. Let $R_{\leq 5}$ be the set of selections containing at most five cans of root beer, and let $L_{\leq 6}$ be the set of selections containing at most six cans of lemonade. The answer to the question can be represented as $N(R_{\leq 5} \cap L_{\leq 6})$. As in part (a), let T be the set of all the selections of fifteen cans in which the soft drink may be any one of the five types assuming that there are at least 15 cans of each type. If you remove all the selections from T that contain at least six cans of root beer or at least seven cans of lemonade, then you are left with all the selections that contain at most five cans of root beer and at most six cans of lemonade. Thus, in the notation of part (a) and Example 9.6.2,

$$N(R_{\leq 5} \cap L_{\leq 6}) = N(T) - N(R_{\geq 6} \cup L_{\geq 7}). \quad (*)$$

Use the inclusion/exclusion rule as follows to compute $N(R_{\geq 6} \cup L_{\geq 7})$:

$$N(R_{\geq 6} \cup L_{\geq 7}) = N(R_{\geq 6}) + N(L_{\geq 7}) - N(R_{\geq 6} \cap L_{\geq 7}).$$

To find $N(R_{\geq 6} \cap L_{\geq 7})$, observe that if at least 6 cans of root beer and at least 7 cans of lemonade are selected, then at most 2 additional cans of soft drink can be chosen from the other three types to make up the total of 15 cans. A selection of two such cans can be represented by a string of 2 $\times$'s and 3 $|$'s, and a selection of one such can can be represented by a string of 1 $\times$ and 3 $|$'s. Hence

$$N(R_{\geq 6} \cap L_{\geq 7}) = \binom{2+3-1}{2} + \binom{1+3-1}{1} = \binom{4}{2} + \binom{3}{1} = 6 + 3 = 9.$$

It follows that

$$\begin{aligned} N(R_{\geq 6} \cup L_{\geq 7}) &= N(R_{\geq 6} + N(L_{\geq 7}) - N(R_{\geq 6} \cap L_{\geq 7}) && \text{by the inclusion/exclusion rule} \\ &= 715 + 495 - 9 && \text{by part (a) and the computation above, and by part (b) of Example 9.6.2} \\ &= 1{,}201. \end{aligned}$$

Putting this result together with equation (*) and the value of $N(T)$ from Example 9.6.2(a) gives that

$$N(R_{\leq 5} \cap L_{\leq 6}) = N(T) - N(R_{\geq 6} \cup L_{\geq 7}) = 3{,}876 - 1{,}201 = 2{,}675.$$

Thus there are 2,675 selections of fifteen soft drinks that contain at most five cans of root beer and at most six cans of lemonade.

17. *Hints:* **a.** The answer is 10,295,472. **b.** See the solution to part (c) of Example 9.6.2. The answer is 9,949,368. **c.** The answer is 9,111,432. **d.** Let T denote the set of all the selections of thirty balloons, assuming that there are at least 30 of each color. Let $R_{\leq 12}$ denote the set of selections from T that contain at most twelve red balloons, let $B_{\leq 8}$ denote the set of selections from T that contain at most eight blue balloons, let $R_{\geq 13}$ denote the set of selections that contain at least thirteen red balloons, and let $B_{\geq 9}$ denote the set of selections that contain at least nine blue balloons. Then the answer to the question can be represented as $N(R_{\leq 12} \cap B_{\leq 8})$. Out of the total of all the balloon selections, if you remove the selections containing at least thirteen red or at least nine blue balloons, then you are left with the selections containing at most twelve red and at most eight blue balloons. Thus $N(R_{\leq 12} \cap B_{\leq 8}) = N(T) - N(R_{\geq 13} \cup B_{\geq 9})$. Compute $N(R_{\geq 13} \cap B_{\geq 9})$, and use the inclusion/exclusion rule to find $N(R_{\geq 13} \cup B_{\geq 9})$.

19. *Hints:* The answers are **a.** 51,128 **b.** 46,761

SECTION 9.7

1. $$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1$$

3. $$\binom{n}{2} = \frac{n!}{(n-2)! \cdot 2!} = \frac{n \cdot (n-1) \cdot (n-2)!}{(n-2)! \cdot 2!} = \frac{n(n-1)}{2}$$

5. Proof: Suppose n and r are nonnegative integers and $r \leq n$. Then

$$\begin{aligned} \binom{n}{r} &= \frac{n!}{r!(n-r)!} && \text{by Theorem 9.5.1} \\ &= \frac{n!}{(n-(n-r))!(n-r)!} && \text{since } n-(n-r) = n-n+r = r \\ &= \frac{n!}{(n-r)!(n-(n-r))!} && \text{by interchanging the factors in the denominator} \\ &= \binom{n}{n-r} && \text{by Theorem 9.5.1.} \end{aligned}$$

6. *Solution 1:* Apply formula (9.7.2) with $m+k$ in place of n. This is legal because $m+k \geq 1$.

Solution 2:

$$\binom{m+k}{m+k-1} = \frac{(m+k)!}{(m+k-1)![(m+k)-(m+k-1)]!} = \frac{(m+k) \cdot (m+k-1)!}{(m+k-1)!(m+k-m-k+1)!} = \frac{(m+k) \cdot (m+k-1)!}{(m+k-1)! \cdot 1!} = m+k$$

10. a. $\binom{6}{2} = \binom{5}{2} + \binom{5}{1} = 10 + 5 = 15$

$\binom{6}{3} = \binom{5}{3} + \binom{5}{2} = 10 + 10 = 20$

$\binom{6}{4} = \binom{5}{4} + \binom{5}{3} = 5 + 10 = 15$

$\binom{6}{5} = \binom{5}{5} + \binom{5}{4} = 1 + 5 = 6$

b. $\binom{7}{3} = \binom{6}{3} + \binom{6}{2} = 20 + 15 = 35$

$\binom{7}{4} = \binom{6}{4} + \binom{6}{3} = 15 + 20 = 35$

$\binom{7}{5} = \binom{6}{5} + \binom{6}{4} = 6 + 15 = 21$

c. Row for $n = 7$: 1 7 21 35 35 21 7 1

13. Proof by mathematical induction: Let the property $P(n)$ be the formula

$$\sum_{i=2}^{n+1} \binom{i}{2} = \binom{n+2}{3}. \quad \leftarrow P(n).$$

Show that P(1) is true:
To prove $P(1)$ we must show that

$$\sum_{i=2}^{1+1} \binom{i}{2} = \binom{1+2}{3}. \quad \leftarrow P(1).$$

Now

$$\sum_{i=2}^{1+1} \binom{i}{2} = \sum_{i=2}^{2} \binom{i}{2} = \binom{2}{2} = 1 = \binom{3}{3} = \binom{1+2}{3},$$

so $P(1)$ is true.

Show that for every integer $k \geq 1$, if $P(k)$ is true, then $P(k+1)$ is true:

Let k be any integer with $k \geq 1$, and suppose that

$$\sum_{i=2}^{k+1} \binom{i}{2} = \binom{k+2}{3}. \quad \leftarrow P(k) \text{ inductive hypothesis}$$

We must show that

$$\sum_{i=2}^{(k+1)+1} \binom{i}{2} = \binom{(k+1)+2}{3},$$

or, equivalently,

$$\sum_{i=2}^{k+2} \binom{i}{2} = \binom{k+3}{3}. \quad \leftarrow P(k+1)$$

Now the left-hand side of $P(k+1)$ is

$$\begin{aligned}
\sum_{i=2}^{k+2} \binom{i}{2} &= \sum_{i=1}^{k+1} \binom{i}{2} + \binom{k+2}{2} && \text{by writing the last term separately} \\
&= \binom{k+2}{3} + \binom{k+2}{2} && \text{by inductive hypothesis} \\
&= \binom{(k+2)+1}{3} && \text{by Pascal's formula} \\
&= \binom{k+3}{3},
\end{aligned}$$

which is the right-hand side of $P(k+1)$ *[as was to be shown]. [Since we have proved the basis step and the inductive step, we conclude that $P(n)$ is true for all $n \geq 1$.]*

14. *Hint:* Use the results of exercises 3 and 13.

17. *Hint:* This follows by letting $m = n = r$ in exercise 16 and using the result of Example 9.7.2.

19. $$1 + 7x + \binom{7}{2}x^2 + \binom{7}{3}x^3 + \binom{7}{4}x^4 + \binom{7}{5}x^5 + \binom{7}{6}x^6 + x^7$$
$$= 1 + 7x + 21x^2 + 35x^3 + 35x^4 + 21x^5 + 7x^6 + x^7$$

21. $$1 + 6(-x) + \binom{6}{2}(-x)^2 + \binom{6}{3}(-x)^3 + \binom{6}{4}(-x)^4 + \binom{6}{5}(-x)^5 + (-x)^6$$
$$= 1 - 6x + 15x^2 - 20x^3 + 15x^4 - 6x^5 + x^6$$

23. $$(p - 2q)^4 = \sum_{k=0}^{4} \binom{4}{k} p^{4-k}(-2q)^k$$
$$= \binom{4}{0}p^4(-2q)^0 + \binom{4}{1}p^3(-2q)^1 + \binom{4}{2}p^2(-2q)^2 + \binom{4}{3}p^1(-2q)^3 + \binom{4}{4}p^0(-2q)^4$$
$$= p^4 - 8p^3q + 24p^2q^2 - 32pq^3 + 16q^4$$

25. $$\left(x + \frac{1}{x}\right)^5 = \sum_{k=0}^{5} \binom{5}{k} x^{5-k}\left(\frac{1}{x}\right)^k$$
$$= \binom{5}{0}x^5\left(\frac{1}{x}\right)^0 + \binom{5}{1}x^4\left(\frac{1}{x}\right)^1$$

$$+\binom{5}{2}x^3\left(\frac{1}{x}\right)^2+\binom{5}{3}x^2\left(\frac{1}{x}\right)^3$$
$$+\binom{5}{4}x^1\left(\frac{1}{x}\right)^4+\binom{5}{5}x^0\left(\frac{1}{x}\right)^5$$
$$=x^5+5x^3+10x+\frac{10}{x}+\frac{5}{x^3}+\frac{1}{x^5}$$

29. The term is $\binom{9}{3}x^6y^3=84x^6y^3$, so the coefficient is 84.

31. The term is $\binom{12}{7}a^5(-2b)^7=792a^5(-128)b^7=-101{,}376a^5b^7$, so the coefficient is $-101{,}376$.

33. The term is $\binom{15}{8}(3p^2)^8(-2q)^7=\binom{15}{8}3^8(-2)^7p^{16}q^7$, so the coefficient is $\binom{15}{8}3^8(-2)^7=-5{,}404{,}164{,}480$.

36. Proof: Let $a=1$, let $b=-1$, and let n be a positive integer. Substitute into the binomial theorem to obtain

$$(1+(-1))^n=\sum_{k=0}^{n}\binom{n}{k}\cdot 1^{n-k}\cdot(-1)^k$$
$$=\sum_{k=0}^{n}\binom{n}{k}(-1)^k \qquad \text{since } 1^{n-k}=1.$$

On the other hand, $(1+(-1))^n=0^n=0$, so

$$0=\sum_{k=0}^{n}\binom{n}{k}(-1)^k$$
$$=\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^n\binom{n}{n}.$$

37. *Hint:* $3=2+1$

38. Proof: Let m be any integer with $m\geq 0$, and apply the binomial theorem with $a=2$ and $b=-1$. The result is

$$1=1^m=(2+(-1))^m=\sum_{i=0}^{m}\binom{m}{i}2^{m-i}(-1)^i$$
$$=\sum_{i=0}^{m}(-1)^i\binom{m}{i}2^{m-i}.$$

41. *Hint:* Apply the binomial theorem with $a=1$ and $b=-\frac{1}{2}$, and analyze the resulting equation when n is even and when n is odd.

43. $\displaystyle\sum_{k=0}^{n}\binom{n}{k}5^k=\sum_{k=0}^{n}\binom{n}{k}1^{n-k}5^k=(1+5)^n=6^n$

45. $\displaystyle\sum_{i=0}^{n}\binom{n}{i}x^i=\sum_{i=0}^{n}\binom{n}{i}1^{n-i}x^i=(1+x)^n$

47. $\displaystyle\sum_{j=0}^{2n}(-1)^j\binom{2n}{j}x^j=\sum_{j=0}^{2n}\binom{2n}{j}1^{2n-j}(-x)^j=(1-x)^{2n}$

51. $\displaystyle\sum_{i=0}^{m}(-1)^j\binom{m}{i}\frac{1}{2^i}=\sum_{i=0}^{m}\binom{m}{i}1^{m-i}\left(-\frac{1}{2}\right)^i$
$$=\left(1-\frac{1}{2}\right)^m=\frac{1}{2^m}$$

53. $\displaystyle\sum_{i=0}^{n}(-1)^i\binom{n}{i}5^{n-i}2^i=\sum_{i=0}^{n}\binom{n}{i}5^{n-i}(-2)^i$
$$=(5-2)^n=3^n$$

55. b. $\displaystyle n(1+x)^{n-1}=\sum_{k=1}^{n}\binom{n}{k}kx^{k-1}$

[The term corresponding to $k=0$ is zero because $\frac{d}{dx}(x^0)=0$.]

c. (i) Substitute $x=1$ in part (b) above to obtain

$$n(1+1)^{n-1}=\sum_{k=1}^{n}\binom{n}{k}k\cdot 1^{k-1}=\sum_{k=1}^{n}\binom{n}{k}k$$
$$=\binom{n}{1}\cdot 1+\binom{n}{2}\cdot 2+\binom{n}{3}\cdot 3+\cdots+\binom{n}{n}n.$$

Dividing both sides by n and simplifying gives

$$2^{n-1}=\frac{1}{n}\left[\binom{n}{1}+2\binom{n}{2}+3\binom{n}{3}+\cdots+n\binom{n}{n}\right].$$

SECTION 9.8

1. By probability axiom 2, $P(\varnothing)=0$.

2. a. By probability axiom 3, $P(A\cup B)=P(A)+P(B)=0.3+0.5=0.8$.

b. Because $A\cup B\cup C=S$ and because A, B, and C are mutually exclusive events, $C=S-(A\cup B)$. Thus, by the formula for the probability of the complement of an event, $P(C)=P((A\cup B)^c)=1-P(A\cup B)=1-0.8=0.2$.

4. By the formula for the probability of a general union of two events, $P(A\cup B)=P(A)+P(B)-P(A\cap B)=0.8+0.7-0.6=0.9$.

7. a. $P(A\cup B)=0.4+0.3=0.7$

b. $P(C)=P((A\cup B)^c)=1-P(A\cup B)=1-0.7=0.3$

c. $P(A\cup C)=0.4+0.3=0.7$

d. $P(A^c)=1-P(A)=1-0.4=0.6$

e. $P(A^c\cap B^c)=P((A\cup B)^c)=1-P(A\cup B)=1-0.7=0.3$

f. $P(A^c\cup B^c)=P((A\cap B)^c)=P(\varnothing^c)=P(S)=1$

9. a. $P(A\cup B)=P(A)+P(B)-P(A\cap B)=0.4+0.5-0.2=0.7$

d. $P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$

11. *Hint:* Since $U \subseteq V$, $V = U \cup (V - U)$

12. *Hint:* For arbitrarily chosen sets U and V, $U \cup (V - U) = U \cup V$.

13. *Hint:* $(A_1 \cup A_2 \cup \ldots \cup A_k) \cap A_{k+1} = \varnothing$ and $A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1} = (A_1 \cup A_2 \cup \ldots \cup A_k) \cup A_{k+1}$.

14. *Solution 1:* The net gain of the grand prize winner is \$2,000,000 − \$2 = \$1,999,998. Each of the 10,000 second prize winners has a net gain of \$20 − \$2 = \$18, and each of the 50,000 third prize winners has a net gain of \$4 − \$2 = \$2. The number of people who do not win anything is 1,500,000 − 1 − 10,000 − 50,000 = 1,439,999, and each of these people has a net loss of \$2. Because all of the 1,500,000 tickets have an equal chance of winning a prize, the expected gain or loss of a ticket is

$$\frac{1}{1500000}(\$1{,}999{,}998 \cdot 1 + \$18 \cdot 10000 + \$2 \cdot 50000 + (-\$2) \cdot 1{,}439{,}999) = -\$0.40.$$

Solution 2: The total income to the lottery organizer is \$2 (per ticket)·1,500,000 (tickets) = \$3,000,000. The payout the lottery organizer must make is \$2,000,000 + (\$20)(10,000) + (\$4)(50,000) = \$2,400,000, so the net gain to the lottery organizer is \$600,000, which amounts to $\frac{\$600{,}000}{1{,}500{,}000} = \$0.40$ per ticket. Thus the expected net loss to a purchaser of a ticket is \$0.40.

16. Let 2_1 and 2_2 denote the two balls with the number 2, and let 5 and 6 denote the other two balls. There are $\binom{6}{2} = 4$ subsets of 2 balls that can be chosen from the urn. The following table shows the sums of the numbers on the balls in each set and the corresponding probabilities:

Subset	Sum s	Probability that the sum = s
$\{2_1, 2_2\}$	4	1/6
$\{2_1, 5\}, \{2_2, 5\}$	7	2/6
$\{2_1, 6\} \{2_2, 6\}$	8	2/6
$\{5, 6\}$	11	1/6

So the expected value is

$$4 \cdot \tfrac{1}{6} + 7 \cdot \tfrac{2}{6} + 8 \cdot \tfrac{2}{6} + 11 \cdot \tfrac{1}{6} = 7.5.$$

19. The following table displays the sum of the numbers showing face up on the dice:

	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Each cell in the table represents an outcome whose probability is $\frac{1}{36}$. Thus the expected value of the sum is

$$2\left(\frac{1}{36}\right) + 3\left(\frac{2}{36}\right) + 4\left(\frac{3}{36}\right) + 5\left(\frac{4}{36}\right) + 6\left(\frac{5}{36}\right) + 7\left(\frac{6}{36}\right) + 8\left(\frac{5}{36}\right) + 9\left(\frac{4}{36}\right) + 10\left(\frac{3}{36}\right) + 11\left(\frac{2}{36}\right) + 12\left(\frac{1}{36}\right) = \frac{252}{36} = 7.$$

20. *Hint:* The answer is about 7.7 cents.

22. *Hint:* The answer is 1.875.

23. *Hint:* To derive P_{20}, use the distinct roots theorem from Section 5.8. The answer is $P_{20} = \frac{5^{300} - 5^{20}}{5^{300} - 1} \cong 1$.

SECTION 9.9

1. $P(B) = \dfrac{P(A \cap B)}{P(A|B)} = \dfrac{1/6}{1/2} = \dfrac{1}{3}$

3. *Hint:* The answer is 60%.

4. a. Proof: Suppose S is any sample space and A and B are any events in S such that $P(B) \neq 0$. Note that

(1) $A \cup A^c = S$ by the complement law for $\cup$.
(2) $B \cap S = B$ by the identity law for $\cap$.
(3) $B \cap (A \cup A^c) = (A \cap B) \cup (A^c \cap B)$ by the distributive law and commutative laws for sets.
(4) $(A \cap B) \cap (A^c \cap B) = \varnothing$ by the complement law for $\cap$ and the commutative and associative laws for sets.

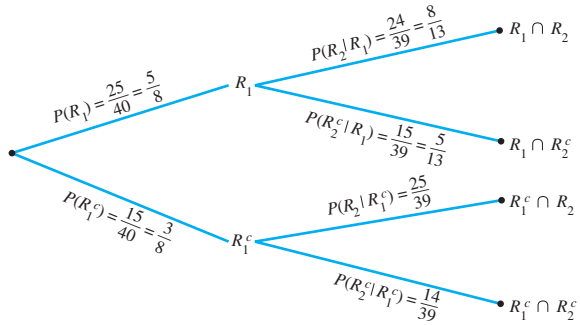
Thus $B = (A \cap B) \cup (A^c \cap B)$, and, by probability axiom 3, $P(B) = P(A \cap B) + P(A^c \cap B)$. Therefore, $P(A^c \cap B) = P(B) - P(A \cap B)$. By definition of conditional probability, it follows that

$$P(A^c|B) = \frac{P(A^c \cap B)}{P(B)} = \frac{P(B) - P(A \cap B)}{P(B)} = 1 - \frac{P(A \cap B)}{P(B)} = 1 - P(A|B).$$

5. *Hints:* (1) $A = (A \cap B) \cup (A \cap B^c)$

(2) The answer is $P(A|B^c) = \dfrac{P(A) - P(A|B)P(B)}{1 - P(B)}$.

6. a. Let R_1 be the probability that the first ball is red, and let R_2 be the probability that the second ball is red. Then R_1^c is the probability that the first ball is not red, and R_2^c is the probability that the second ball is not red. The tree diagram shows the various relations among the probabilities.



Then

$$P(R_1 \cap R_2) = P(R_2|R_1)\cdot P(R_1) = \frac{8}{13}\cdot\frac{5}{8} = \frac{5}{13} \cong 38.5\%$$

$$P(R_1 \cap R_2^c) = P(R_2^c|R_1)\cdot P(R_1) = \frac{5}{13}\cdot\frac{5}{8} = \frac{25}{104} \cong 24\%,$$

$$P(R_1^c \cap R_2) = P(R_2|R_1^c)\cdot P(R_1^c) = \frac{25}{39}\cdot\frac{3}{8} = \frac{25}{104} \cong 24\%,$$

$$P(R_1^c \cap R_2^c) = P(R_2^c|R_1^c)\cdot P(R_1^c) = \frac{14}{39}\cdot\frac{3}{8} = \frac{14}{104} \cong 13.5\%$$

So the probability that both balls are red is $5/13$, the probability that the first ball is red and the second is not is $25/104$, the probability that the first ball is not red and the second ball is red is $25/104$, and the probability that neither ball is red is $14/104$.

b. Note that

$$R_2 = (R_2 \cap R_1) \cup (R_2 \cap R_1^c) \quad \text{and} \quad (R_2 \cap R_1) \cap (R_2 \cap R_1^c) = \varnothing$$

Thus the probability that the second ball is red is

$$P(R_2) = P(R_2 \cap R_1) + P(R_2 \cap R_1^c) = \frac{5}{13} + \frac{25}{104} = \frac{65}{104} \cong 62.5\%.$$

c. If exactly one ball is red, then either the first ball is red and the second is not or the first ball is not red and the second is red, and these possibilities are mutually exclusive. Thus

$$P(\text{exactly one ball is red}) = P(R_1 \cap R_2^c) + P(R_1^c \cap R_2) = \frac{25}{104} + \frac{25}{104} = \frac{50}{104} = \frac{25}{52} \cong 48.1\%.$$

The probability that both balls are red is $P(R_1 \cap R_2) = \frac{5}{13} \cong 38.5\%$. Then

$$P(\text{at least one ball is red}) = P(\text{exactly one ball is red}) + P(\text{both balls are red}) = \frac{25}{52} + \frac{5}{13} = \frac{45}{52} \cong 86.5\%.$$

8. a. Let W_1 be the event that a woman is chosen on the first draw,

W_2 be the event that a woman is chosen on the second draw,

M_1 be the event that a man is chosen on the first draw,

M_2 be the event that a man is chosen on the second draw.

Then $P(W_1) = \frac{3}{10}$ and $P(W_2|W_1) = \frac{2}{9}$, and thus

$$P(W_1 \cap W_2) = P(W_2|W_1)P(W_1) = \tfrac{2}{9}\cdot\tfrac{3}{10} = \tfrac{1}{15} = 6\tfrac{2}{3}\%.$$

c. *Hint:* The answer is $\frac{7}{15} = 46\frac{2}{3}\%$.

9. *Hint:* Use the facts that $P(B_k|A) = \frac{P(B_k \cap A)}{P(A)}$ and that $(A \cap B_1) \cup (A \cap B_2) = A$.

11. a. Let U_1 be the event that the first urn is chosen, U_2 the event that the second urn is chosen, and B the event that the chosen ball is blue. Then

$$P(B|U_1) = \frac{12}{19} \quad \text{and} \quad P(B|U_2) = \frac{8}{27}.$$

$$P(B \cap U_1) = P(B|U_1)P(U_1) = \frac{12}{19}\cdot\frac{1}{2} = \frac{12}{38}.$$

Also

$$P(A \cap U_2) = P(B|U_2)P(U_2) = \frac{8}{27}\cdot\frac{1}{2} = \frac{8}{54}.$$

Now B is the disjoint union of $B \cap U_1$ and $B \cap U_2$. So

$$P(B)P(U_1|B) = P(B \cap U_1) + P(B \cap U_2)$$
$$= \frac{12}{38} + \frac{8}{54} \cong 46.4\%.$$

Thus the probability that the chosen ball is blue is approximately 46.4%.

b. Given that the chosen ball is blue, the probability that it came from the first urn is $P(U_1|B)$. By Bayes' theorem and the computations in part (a),

$$P(U_1|B) = \frac{P(B|U_1)P(U_1)}{P(B|U_1)P(U_1) + P(B|U_2)P(U_2)}$$
$$= \frac{(12/19)(0.5)}{(12/19)(0.5) + (8/27)(0.5)} \cong 68.1\%$$

13. *Hint:* The answers to parts (a) and (b) are approximately 52.9% and 54.0%, respectively.

14. Let A be the event that a randomly chosen person tests positive for drugs, let B_1 be the event that a randomly chosen person uses drugs, and let B_2 be the event that a randomly chosen person does not use drugs. Then A^c is the event that a randomly chosen person does not test positive for drugs, and $P(B_1) = 0.04$, $P(B_2) = 0.96$, $P(A|B_2) = 0.03$, and $P(A^c|B_1) = 0.02$. Hence $P(A|B_1) = 0.98$ and $P(A^c|B_2) = 0.97$.

a. $$P(B_1|A) = \frac{P(A|B_1)P(B_1)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2)}$$
$$= \frac{(0.97)(0.04)}{(0.97)(0.04) + (0.03)(0.96)} \cong 57.6\%$$

b. $$P(B_2|A^c) = \frac{P(A^c|B_2)P(B_2)}{P(A^c|B_1)P(B_1) + P(A^c|B_2)P(B_2)}$$
$$= \frac{(0.98)(0.96)}{(0.02)(0.04) + (0.98)(0.96)} \cong 99.9\%$$

16. *Hint:* The answers to parts (a) and (b) are 11.25% and $21\frac{1}{3}\%$, respectively.

17. Proof: Suppose A and B are events in a sample space S, and $P(A|B) = P(A) \neq 0$. Then

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(A|B)P(B)}{P(A)}$$
$$= \frac{P(A)P(B)}{P(A)} = P(B).$$

19. As in Example 6.9.1, the sample space is the set of all 36 outcomes obtained from rolling the two dice and noting the numbers showing face up on each. Let A be the event that the number on the blue die is 2 and B the event that the number on the gray die is 4 or 5. Then

$$A = \{21, 22, 23, 24, 25, 26\},$$
$$B = \{14, 24, 34, 44, 54, 64, 15, 25, 35, 45, 55, 65\}, \quad \text{and}$$
$$A \cap B = \{24, 25\}.$$

Since the dice are fair (so all outcomes are equally likely), $P(A) = \frac{6}{36}$, $P(B) = \frac{12}{36}$, and $P(A \cap B) = \frac{2}{36}$. By definition of conditional probability,

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{2}{36}}{\frac{12}{36}} = \frac{1}{6} \quad \text{and}$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{2}{36}}{\frac{6}{36}} = \frac{1}{3}.$$

Now $P(A) = \frac{6}{36} = \frac{1}{6}$ and $P(B) = \frac{12}{36} = \frac{1}{3}$, and hence $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

23. Let A be the event that the student answers the first question correctly, and let B be the event that the student answers the second question correctly. Because two choices can be eliminated on the first question, $P(A) = \frac{1}{3}$, and because no choices can be eliminated on the second question, $P(B) = \frac{1}{5}$. Thus $P(A^c) = \frac{2}{3}$ and $P(B^c) = \frac{4}{5}$.

a. *Hint:* The probability that the student answers both questions correctly is

$$P(A \cap B) = P(A)P(B) = \frac{1}{3} \cdot \frac{1}{5} = \frac{1}{15} = 6\frac{2}{3}\%.$$

b. The probability that the student answers exactly one question correctly is

$$P((A \cap B^c) \cup (A^c \cap B))$$
$$= P(A \cap B^c) + P(A^c \cap B)$$
$$= P(A)P(B^c) + P(A^c)P(B)$$
$$= \frac{1}{3} \cdot \frac{4}{5} + \frac{2}{3} \cdot \frac{1}{5} = \frac{6}{15} = \frac{2}{5} = 40\%.$$

c. One solution is to say that the probability that the student answers both questions incorrectly is $P(A^c \cap B^c)$, and $P(A^c \cap B^c) = P(A^c)P(B^c)$ by the result of exercise 22. Thus the answer is

$$P(A^c)P(B^c) = \frac{2}{3} \cdot \frac{4}{5} = \frac{8}{15} = 53\frac{1}{3}\%.$$

Another solution uses the fact that the event that the student answers both questions incorrectly is the complement of the event that the student answers at least one question correctly. Thus, by the results of parts (a) and (b), the answer is $1 - \left(\frac{1}{15} + \frac{2}{5}\right) = \frac{8}{15} = 53\frac{1}{3}\%$.

25. Let H_i be the event that the result of toss i is heads, and let T_i be the event that the result of toss i is tails. Then $P(H_i) = 0.7$ and $P(T_i) = 0.3$ for $i = 1$ and 2.

b. The probability of obtaining exactly one head is

$$\begin{aligned} P((H_1 \cap T_2) \cup (T_1 \cap H_2)) &= P(H_1 \cap T_2) + P(T_1 \cap H_2) \\ &= P(H_1)P(T_2) + P(T_1)P(H_2) \\ &= (0.7)(0.3) + (0.3)(0.7) = 42\%. \end{aligned}$$

27. *Hint:* The answer is $\frac{1}{2}$.

28. a. P(seven heads)

$$= \begin{bmatrix} \text{the number of different} \\ \text{ways seven heads can} \\ \text{be obtained in ten tosses} \end{bmatrix} (0.7)^7(0.3)^3$$

$$= 120(0.7)^7(0.3)^3 \cong 0.267 = 26.7\%$$

29. a. P(none is defective)

$$= \begin{bmatrix} \text{the number of different} \\ \text{ways of having 0 defective} \\ \text{items in the sample of 10} \end{bmatrix} (0.03)^0(0.97)^{10}$$

$$= 1 \cdot (0.3)^0(0.97)^{10} \cong 0.737 = 73.7\%$$

30. b. The probability that a woman will have at least one false positive result over a period of ten years is $1 - (0.96)^{10} \cong 33.5\%$.

31. a. P(none is male) $\cong 1.3\%$

b. P(at least one is male) = $1 - P$(none is male) $\cong 1 - 0.013 = 98.7\%$

34. *Hint:* $P(Y) = P(Y \cap X) + P(Y \cap X^c)$

SECTION 10.1

1. a. trail (no repeated edge), not a path (has a repeated vertex, v_1), not a circuit

b. walk, not a trail (has a repeated edge, e_9), not a circuit

c. closed walk (starts and ends at the same vertex), trail (no repeated edge since no edge), not a path or a circuit (since no edge)

d. circuit, not a simple circuit (repeated vertex, v_4)

e. closed walk (starts and ends at the same vertex but has repeated edges, $\{v_2, v_3\}$ and $\{v_3, v_4\}$)

f. path

3. a. No. The notation $v_1v_2v_1$ could equally well refer to $v_1e_1v_2e_2v_1$ or to $v_1e_2v_2e_1v_1$, which are different walks.

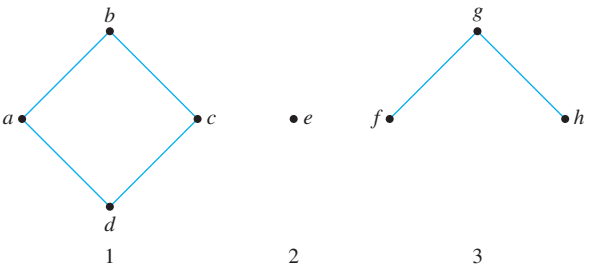
4. a. Three. (There are three ways to choose the middle edge.)

b. $3! + 3 = 9$ (The three paths from part (a) are also trails, and there are an additional 3! trails with vertices $v_1, v_2, v_3, v_2, v_3, v_4$. The reason is that from v_2 there are 3 choices of an edge to go to v_3, then 2 choices of a different edge to go back to v_2, and then 1 choice of a different edge to return to v_3.

c. Infinitely many. (Since a walk may have repeated edges, a walk from v_1 to v_4 may contain an arbitrarily large number of repetitions of edges joining a pair of vertices along the way.)

6. a. $\{v_1, v_3\}$, $\{v_2, v_3\}$, $\{v_4, v_3\}$, and $\{v_5, v_3\}$ are all the bridges.

8. a. Three connected components, as shown in the next column.



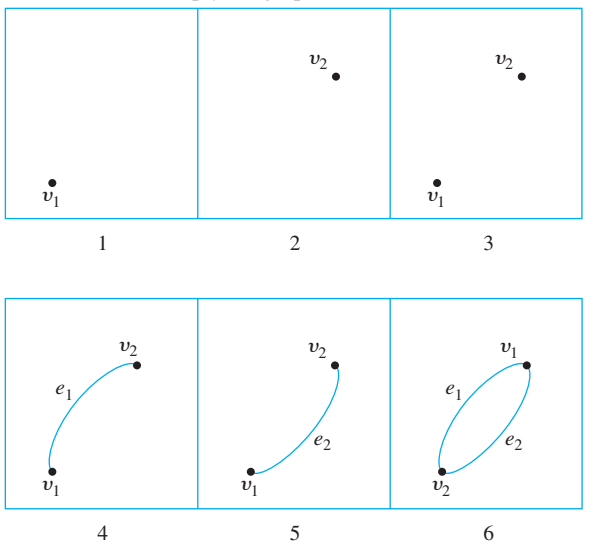
9. a. No. This graph has two vertices of odd degree, whereas all vertices of a graph with an Euler circuit have even degree.

12. One Euler circuit is $e_4e_5e_6e_3e_2e_7e_8e_1$.

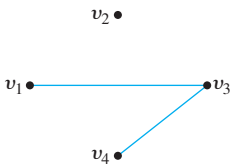
14. One Euler circuit is *iabihbchgcdgfdefi*.

19. There is an Euler trail since deg(u) and deg(w) are odd, all other vertices have positive even degree, and the graph is connected. One Euler trail is $uv_1v_0v_7uv_2v_3v_4v_2v_6v_4wv_5v_6w$.

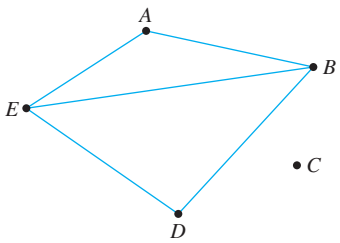
23. a. The nonempty subgraphs are as follows:



24. a.



26. b.



27. *Hint:* Consider the graph obtained by taking the vertices and edges of G plus all the edges of G'.

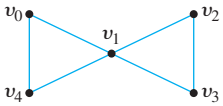
29. $v_0v_7v_1v_2v_3v_5v_6v_0$

31. *Hint:* See the solution to Example 10.1.9.

32. Here is one sequence of reasoning you could use: Call the given graph G, and suppose G has a Hamiltonian circuit. Then G has a subgraph H that satisfies conditions (1)–(4) of Proposition 10.1.6. Since the degree of b in G is 4 and every vertex in H has degree 2, two edges incident on b must be removed from G to create H. Edge $\{a, b\}$ cannot be removed because doing so would result in vertex d having degree less than 2 in H. Similar reasoning shows that edge $\{b, c\}$ cannot be removed either. So edges $\{b, i\}$ and $\{b, e\}$ must be removed from G to create H. Because vertex e must have degree 2 in H and because edge $\{b, e\}$ is not in H, both edges $\{e, d\}$ and $\{e, f\}$ must be in H. Similarly, since both vertices c and g must have degree 2 in H, edges $\{c, d\}$ and $\{g, d\}$ must also be in H. But then three edges incident on d, namely, $\{e, d\}$, $\{c, d\}$, and $\{g, d\}$, must all be in H, which contradicts the fact that vertex d must have degree 2 in H.

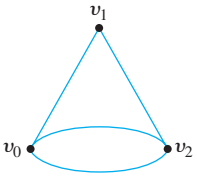
34. *Hint:* This graph does not have a Hamiltonian circuit.

38. *Partial answer:*



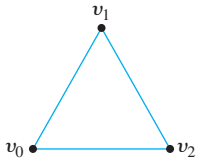
This graph has an Euler circuit $v_0v_1v_2v_3v_1v_4v_0$ but no Hamiltonian circuit.

39. *Partial answer:*



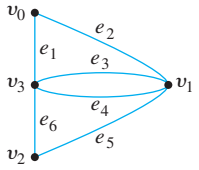
This graph has a Hamiltonian circuit $v_0v_1v_2v_0$ but no Euler circuit.

40. *Partial answer:*



The walk $v_0v_1v_2v_0$ is both an Euler circuit and a Hamiltonian circuit for this graph.

41. *Partial answer:*

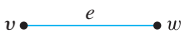


This graph has the Euler circuit $e_1e_2e_3e_4e_5e_6$ and the Hamiltonian circuit $v_0v_1v_2v_3v_0$. These are not the same.

43. a. Proof: Suppose G is a graph and W is a walk in G that contains a repeated edge e. Let v and w be the endpoints of e. In case $v = w$, then v is a repeated vertex of W. In case $v \neq w$, then one of the following must occur: (1) W contains two copies of vew or of wev (for instance, W might contain a section of the form $vewe'vew$, as illustrated below); (2) W contains separate sections of the form vew and wev (for instance, W might contain a section of the form $vewe'wev$, as illustrated below); or (3) W contains a section of the form $vewev$ or of the form $wevew$ (as illustrated below). In cases (1) and (2), both vertices v and w are repeated, and in case (3), one of v or w is repeated. In all cases, there is at least one vertex in W that is repeated.

(1)

(2)

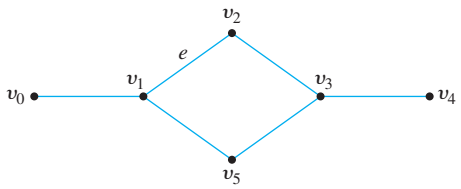


(3)

44. Proof: Suppose G is a connected graph and v and w are any particular but arbitrarily chosen vertices of G. *[We must show that u and v can be connected by a path.]* Since G is connected, there is a walk from v to w. If the walk contains a repeated vertex, then delete the portion of the walk from the first occurrence of the vertex to its next occurrence. (For example, in the walk $ve_1v_2e_5v_7e_6v_2e_3w$, the vertex v_2 occurs twice. Deleting the portion of the walk from one occurrence to the next

gives $ve_1v_2e_3w$.) If the resulting walk still contains a repeated vertex, do the above deletion process another time. Then check again for a repeated vertex. Continue in this way until all repeated vertices have been deleted. (This must occur eventually, since the total number of vertices is finite.) The resulting walk connects v to w but has no repeated vertex. By exercise 43(b), it has no repeated edge either. Hence it is a path from v to w.

46. The graph below contains a circuit, any edge of which can be removed without disconnecting the graph. For instance, if edge e is removed, then the following walk can be used to go from v_1 to v_2: $v_1v_5v_3v_2$.



48. *Hint:* Look at the answer to exercise 46 and use the fact that all graphs have a finite number of edges.

50. Proof: Let G be a connected graph and let C be a circuit in G. Let G' be the subgraph obtained by removing all the edges of C from G and also any vertices that become isolated when the edges of C are removed. *[We must show that there exists a vertex v such that v is in both C and G'.]* Pick any vertex v of C and any vertex w of G'. Since G is connected, there is a path from v to w (by Lemma 10.1.1(a)):

$$v = v_0e_1v_1e_2v_2 \ldots v_{i-1}e_iv_ie_{i+1}v_{i+1} \ldots v_{n-1}e_nv_n = w.$$
$$\uparrow \text{ in } C \qquad \uparrow \text{ in } C \quad \uparrow \text{ not in } C \qquad \uparrow \text{ in } G'$$

Let i be the largest subscript such that v_i is in C. If $i = n$, then $v_n = w$ is in C and also in G', and we are done. If $i < n$, then v_i is in C and v_{i+1} is not in C. This implies that e_{i+1} is not in C (for if it were, both endpoints would be in C by definition of circuit). Hence when G' is formed by removing the edges and resulting isolated vertices from G, then e_{i+1} is not removed. That means that v_i does not become an isolated vertex, so v_i is not removed either. Hence v_i is in G'. Consequently, v_i is in both C and G' *[as was to be shown].*

51. Proof: Suppose G is a graph with an Euler circuit. If G has only one vertex, then G is automatically connected. If v and w are any two vertices of G, then v and w each appear at least once in the Euler circuit (since an Euler circuit contains every vertex of the graph). The section of the circuit between the first occurrence of one of v or w and the first occurrence of the other is a walk from one of the two vertices to the other. Since the choice of v and w was arbitrary, given any two vertices in G there is a walk from one to the other. So, by definition, G is connected.

56. b. *Hint:* Divide the proof into three parts. (1) Show that if G is any graph containing a closed walk with an odd number of edges, then G contains a circuit with an odd number of edges. (2) Show that if G is any connected graph that does not have a circuit with an odd number of edges, then G is bipartite. (3) Show that if G is any graph with at least two vertices and is such that G does not have a circuit with an odd number of edges, then G is bipartite.

SECTION 10.2

1. a. Equating corresponding entries shows that

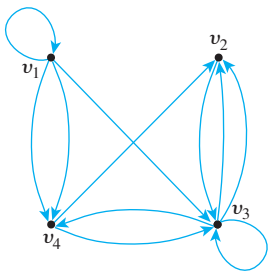
$$\begin{aligned} a + b &= 1 \\ a - c &= 0 \\ c &= -1 \\ b - a &= 3. \end{aligned}$$

Thus $a - c = a - (-1) = 0$, and so $a = -1$. Consequently, $a + b = (-1) + b = 1$, and hence $b = 2$. The last equation should be checked to make sure the answer is consistent: $b - a = 2 - (-1) = 3$, which agrees.

2. a.

	v_1	v_2	v_3
v_1	0	1	1
v_2	1	0	0
v_3	0	0	0

3. a.



Any labels may be applied to the edges because the adjacency matrix does not determine edge labels.

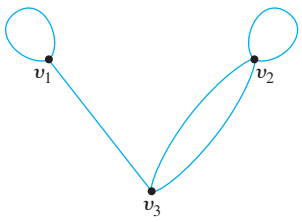
4. a.

	v_1	v_2	v_3	v_4
v_1	0	0	1	1
v_2	0	0	2	0
v_3	1	2	0	0
v_4	1	0	0	1

c.

	v_1	v_2	v_3	v_4
v_1	0	1	1	1
v_2	1	0	1	1
v_3	1	1	0	1
v_4	1	1	1	0

5. a.



Any labels may be applied to the edges because the adjacency matrix does not determine edge labels.

6. a. The graph is connected.

8. a. $2 \cdot 1 + (-1) \cdot 3 = -1$

9. a. $\begin{bmatrix} 3 & -3 & 12 \\ 1 & -5 & 2 \end{bmatrix}$ **d.** $\begin{bmatrix} 7 & 0 \\ 0 & 7 \end{bmatrix}$

10. a. No product. (**A** has three columns, and **B** has two rows.)

b. $\mathbf{BA} = \begin{bmatrix} -2 & -2 & 2 \\ 1 & -5 & 2 \end{bmatrix}$

f. $\mathbf{B}^2 = \begin{bmatrix} 4 & 0 \\ 1 & 9 \end{bmatrix}$

i. $\mathbf{AC} = \begin{bmatrix} 2 & -1 \\ -5 & -2 \end{bmatrix}$

12. One among many possible examples is

$$\mathbf{A} = \mathbf{B} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

14. *Hint:* If the entries of the $m \times m$ identity matrix are denoted by δ_{ik}, then $\delta_{ik} = \begin{cases} 0 & \text{if } i \neq k \\ 1 & \text{if } i = k. \end{cases}$

The ijth entry of $\mathbf{IA}$ is $\sum_{k=1}^{m} \delta_{ik}\mathbf{A}_{kj}$.

15. Proof: Suppose **A** is an $m \times m$ symmetric matrix. Then for all integers i and j with $1 \leq i, j \leq m$,

$$(\mathbf{A}^2)_{ij} = \sum_{k=1}^{m} \mathbf{A}_{ik}\mathbf{A}_{kj} \quad \text{and} \quad (\mathbf{A}^2)_{ji} = \sum_{k=1}^{m} \mathbf{A}_{jk}\mathbf{A}_{ki}.$$

But since **A** is symmetric, $\mathbf{A}_{ik} = \mathbf{A}_{ki}$ and $\mathbf{A}_{kj} = \mathbf{A}_{jk}$ for all i, j, and k, and thus $\mathbf{A}_{ik}\mathbf{A}_{kj} = \mathbf{A}_{jk}\mathbf{A}_{ki}$ *[by the commutative law for multiplication of real numbers]*. Hence $(\mathbf{A}^2)_{ij} = (\mathbf{A}^2)_{ji}$ for all integers i and j with $1 \leq i, j \leq m$.

17. Proof (by mathematical induction): Let the property $P(n)$ be the equation $\mathbf{A}^n\mathbf{A} = \mathbf{A}\mathbf{A}^n$.

Show that P(1) is true:
We must show that $\mathbf{A}^1\mathbf{A} = \mathbf{A}\mathbf{A}^1$. But this is true because $\mathbf{A}^1 = \mathbf{A}$ and $\mathbf{A}\mathbf{A} = \mathbf{A}\mathbf{A}$.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:
Let k be any integer such that $k \geq 1$, and suppose that $\mathbf{A}^k\mathbf{A} = \mathbf{A}\mathbf{A}^k$. *[This is the inductive hypothesis.]* We must show that $\mathbf{A}^{k+1}\mathbf{A} = \mathbf{A}\mathbf{A}^{k+1}$. But

$$\begin{aligned} \mathbf{A}^{k+1}\mathbf{A} &= (\mathbf{A}\mathbf{A}^k)\mathbf{A} && \text{by definition of matrix power} \\ &= \mathbf{A}(\mathbf{A}^k\mathbf{A}) && \text{by exercise 16} \\ &= \mathbf{A}(\mathbf{A}\mathbf{A}^k) && \text{by inductive hypothesis} \\ &= \mathbf{A}\mathbf{A}^{k+1} && \text{by definition of matrix power.} \end{aligned}$$

19. a. $\mathbf{A}^2 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 3 & 3 \\ 3 & 2 & 2 \\ 3 & 2 & 5 \end{bmatrix}$

$$\mathbf{A}^3 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}\begin{bmatrix} 6 & 3 & 3 \\ 3 & 2 & 2 \\ 3 & 2 & 5 \end{bmatrix} = \begin{bmatrix} 15 & 9 & 15 \\ 9 & 5 & 8 \\ 15 & 8 & 8 \end{bmatrix}$$

20. a. 2 since $(\mathbf{A}^2)_{23} = 2$
b. 3 since $(\mathbf{A}^2)_{34} = 3$
c. 6 since $(\mathbf{A}^3)_{14} = 6$
d. 17 since $(\mathbf{A}^3)_{23} = 17$

22. b. *Hint:* If G is bipartite, then its vertices can be partitioned into two sets V_1 and V_2 so that no vertices in V_1 are connected to each other by an edge and no vertices in V_2 are connected to each other by an edge. Label the vertices in V_1 as $v_1, v_2, \ldots, v_k$ and label the vertices in V_2 as $v_{k+1}, v_{k+2}, \ldots, v_n$. Now look at the matrix of G formed according to the given vertex labeling.

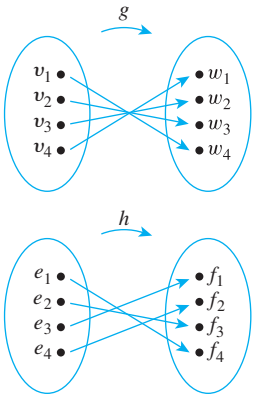
23. b. *Hint:* Consider the ijth entry of

$$\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \cdots + \mathbf{A}^n.$$

If G is connected, then given the vertices v_i and v_j, there is a walk connecting v_i and v_j. If this walk has length k, then by Theorem 10.2.2, the ijth entry of $\mathbf{A}^k$ is not equal to 0. Use the facts that all entries of each power of **A** are nonnegative and that a sum of nonnegative numbers is positive provided that at least one of the numbers is positive.

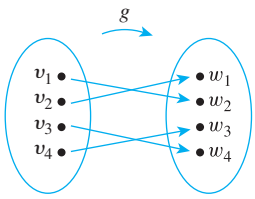
SECTION 10.3

1. The graphs are isomorphic. One way to define the isomorphism is as follows:



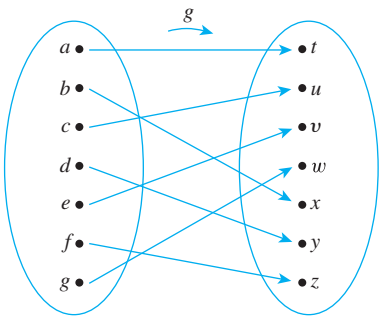
2. The graphs are not isomorphic. G has five vertices and G' has six.

6. The graphs are isomorphic. One isomorphism is the following:

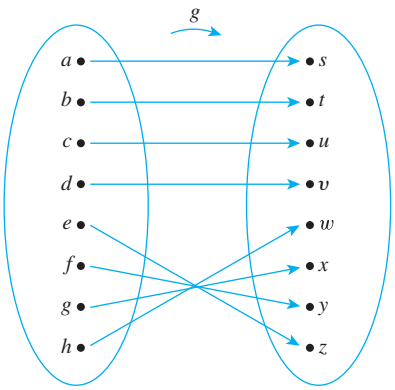


8. The graphs are not isomorphic. G has a simple circuit of length 3; G' does not.

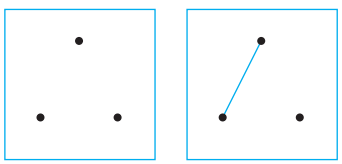
10. The graphs are isomorphic. One way to define the isomorphism is as follows:



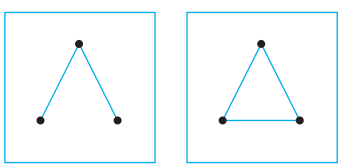
12. The graphs are isomorphic. One isomorphism is the following:



14.

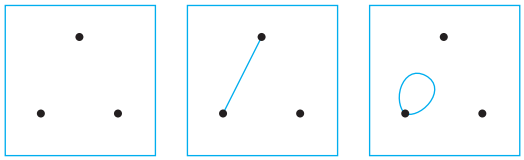


1 2

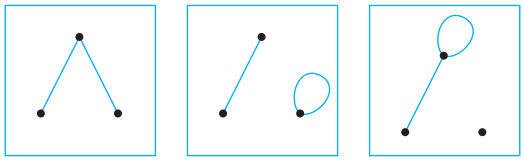


3 4

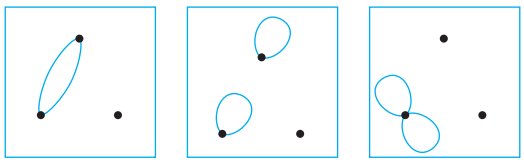
16.



1 2 3



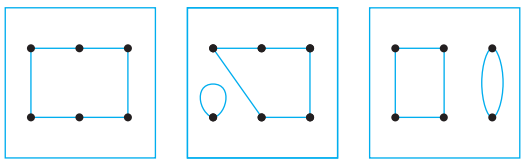
4 5 6



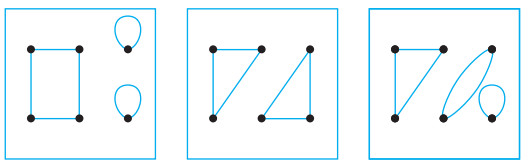
7 8 9

18. *Hint:* There are 20.

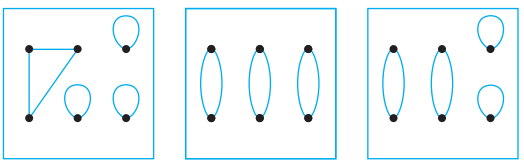
19.



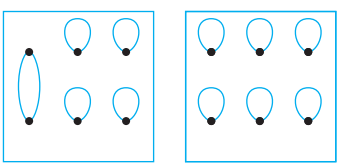
1 2 3



4 5 6



7 8 9



10 11

21. Proof: Suppose G and G' are isomorphic graphs and G has n vertices, where n is a nonnegative integer.

[We must show that G' has n vertices.] By definition of graph isomorphism, there is a one-to-one correspondence $g: V(G) \to V(G')$ sending vertices of G to vertices of G'. Since $V(G)$ is a finite set and g is a one-to-one correspondence, the number of vertices in $V(G')$ equals the number of vertices in $V(G)$. Hence G' has n vertices *[as was to be shown]*.

23. Proof: Suppose G and G' are isomorphic graphs and suppose G has a circuit C of length k, where k is a nonnegative integer. Let C be $v_0e_1v_1e_2 \ldots e_kv_k(=v_0)$. By definition of graph isomorphism, there are one-to-one correspondences $g: V(G) \to V(G')$ and $h: E(G) \to E(G')$ that preserve the edge-endpoint functions in the sense that for each v in $V(G)$ and each e in $E(G)$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$. Let C' be $g(v_0)h(e_1)g(v_1)h(e_2) \ldots . h(e_k)g(v_k)(=g(v_0))$. Then C' is a circuit of length k in G'. The reasons are that (1) because g and h preserve the edge-endpoint functions, both $g(v_i)$ and $g(v_{i+1})$ are incident on $h(e_{i+1})$ for each $i = 0, 1, \ldots, k-1$, and so C' is a walk from $g(v_0)$ to $g(v_0)$, and (2) since C is a circuit, then $e_1, e_2, \ldots, e_k$ are distinct, and since h is a one-to-one correspondence, $h(e_1), h(e_2), \ldots, h(e_k)$ are also distinct, which implies that C' has k distinct edges. Therefore, G' has a circuit C of length k.

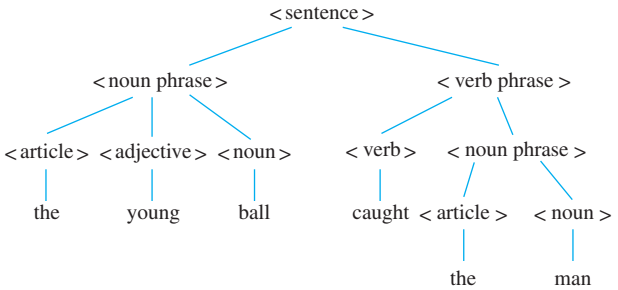
25. *Hint:* Suppose G and G' are isomorphic and G has m vertices of degree k; call them $v_1, v_2, \ldots, v_m$. Since G and G' are isomorphic, there are one-to-one correspondences g: $V(G) \to V(G')$ and $h: E(G) \to E(G')$. Show that $g(v_1), g(v_2), \ldots, g(v_m)$ are m distinct vertices of G', each of which has degree k.

27. *Hint:* Suppose G and G' are isomorphic and G is connected. To show that G' is connected, suppose w and x are any two vertices of G'. Show that there is a walk connecting w with x by finding a walk connecting the corresponding vertices in G.

SECTION 10.4

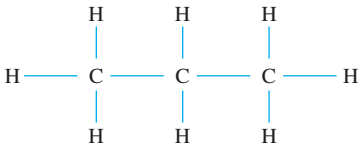
1. a. Math 110

2. a.



3. *Hint:* The answer is $2n - 2$. To obtain this result, use the relationship between the total degree of a graph and the number of edges of the graph.

4. a.



d. *Hint:* Each carbon atom in G is bonded to four other atoms in G, because otherwise an additional hydrogen atom could be bonded to it, and this would contradict the assumption that G has the maximum number of hydrogen atoms for its number of carbon atoms. Also each hydrogen atom is bonded to exactly one carbon atom in G, because otherwise G would not be connected.

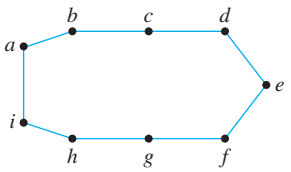
5. *Hint:* Revise the algorithm given in the proof of Lemma 10.4.1 to keep track of which vertex and edge were chosen in step 1 (by, say, labeling them v_0 and e_0). Then after one vertex of degree 1 is found, return to v_0 and search for another vertex of degree 1 by moving along a path outward from v_0 starting with another edge incident on v_0. Such an edge exists because v_0 has degree at least 2.

7. a. Internal (or branch) vertices: v_2, v_3, v_4, v_6

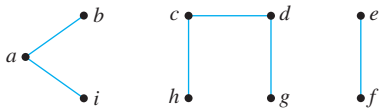
Leaves (or terminal vertices: v_1, v_5, v_7

8. Any tree with nine vertices has eight edges, not nine. Thus there is no tree with nine vertices and nine edges.

9. One such graph is

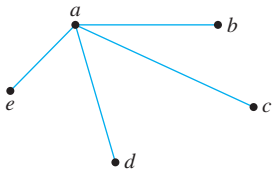


10. One such graph is



11. There is no tree with six vertices and a total degree of 14. Any tree with six vertices has five edges and hence, by the handshake theorem (Theorem 4.9.1) it has a total degree of 10, not 14.

12. One such tree is shown.



13. No such graph exists. By Theorem 10.4.4, a connected graph with six vertices and five edges is a tree. Hence such a graph cannot have a nontrivial circuit.

14.

22. Yes. Since it is connected and has 12 vertices and 11 edges, by Theorem 10.4.4 it is a tree. It follows from Lemma 10.5.1 that it has vertex of degree 1.

25. Suppose there were a connected graph with eight vertices and six edges. Either the graph itself would be a tree or edges could be eliminated from its circuits to obtain a tree. In either case, there would be a tree with eight vertices and six or fewer edges. But by Theorem 10.4.2, a tree with eight vertices has seven edges, not six or fewer. This contradiction shows that the supposition is false, so there is no connected graph with eight vertices and six edges.

26. *Hint:* See the answer to exercise 25.

27. Yes. Suppose G is a circuit-free graph with ten vertices and nine edges. Let $G_1, G_2, \ldots, G_k$ be the connected components of G. *[To show that G is connected, we will show that $k = 1$.]* Each G_i is a tree since each G_i is connected and circuit-free. For each $i = 1, 2, \ldots, k$, let G_i have n_i vertices. Note that since G has ten vertices in all,

$$n_1 + n_2 + \cdots n_k = 10.$$

By Theorem 10.4.2,

$$G_1 \text{ has } n_1 - 1 \text{ edges},$$
$$G_2 \text{ has } n_2 - 1 \text{ edges},$$
$$\vdots$$
$$G_k \text{ has } n_k - 1 \text{ edges}.$$

So the number of edges of G equals

$$\begin{aligned}&(n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1)\\ &\quad = (n_1 + n_2 + \cdots + n_k) - \underbrace{(1 + 1 + \cdots + 1)}_{k \text{ 1's}}\\ &\quad = 10 - k.\end{aligned}$$

But we are given that G has nine edges. Hence $10 - k = 9$, and so $k = 1$. Thus G has just one connected component, G_1, and so G is connected.

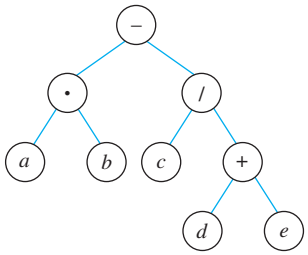
28. *Hint:* See the answer to exercise 27 and the proof of Corollary 10.4.5.

31. b. *Hint:* There are six.

SECTION 10.5

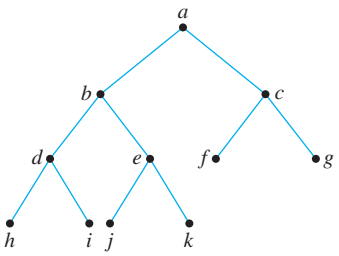
1. a. 3 **b.** 0 **c.** 5 **d.** u, v
e. d **f.** k, l **g.** m, s, t, x, y **h.** 12

3. a.



Exercises 4 and 8–10 have other answers in addition to the ones shown.

4.

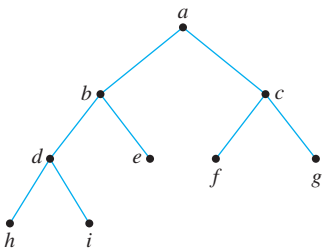


5. There is no full binary tree with the given properties because any full binary tree with five internal vertices has six leaves, not seven.

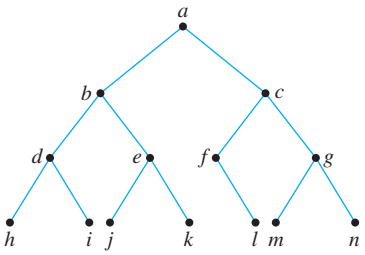
6. Any full binary tree with four internal vertices has five leaves for a total of nine—not seven—vertices in all. Thus there is no full binary tree with the given properties.

7. There is no full binary tree with 12 vertices because any full binary tree has $2k + 1$ vertices, where k is the number of internal vertices. But $2k + 1$ is always odd, and 12 is even.

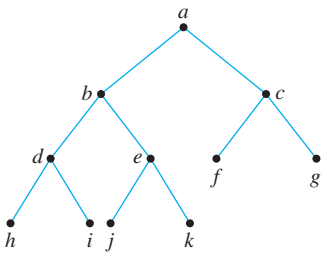
8.



9.



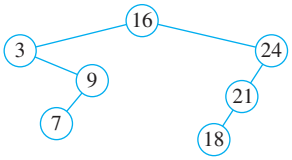
10.



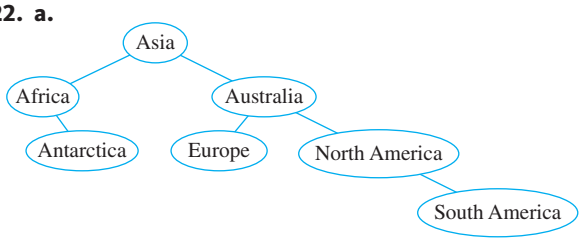
11. There is no binary tree that has height 3 and nine leaves because any binary tree of height 3 has at most $2^3 = 8$ leaves.

20. a. The height of the tree $\geq \log_2 25 \cong 4.6$. So since the height of any tree is an integer, the height of this tree must be at least 5.

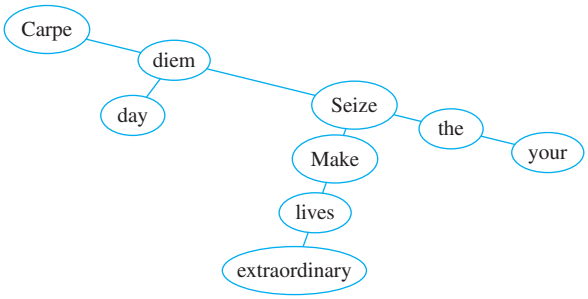
21. a.



22. a.

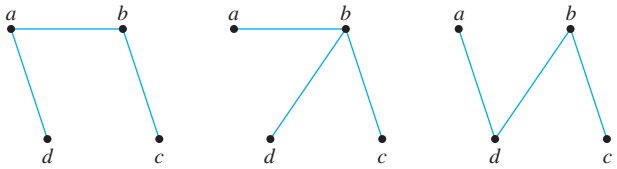


23.

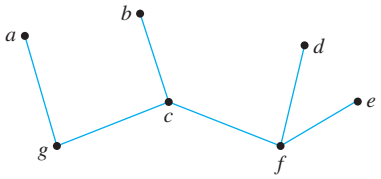


SECTION 10.6

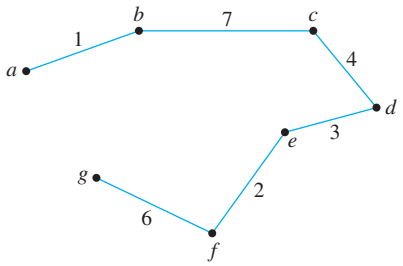
1.



3. One of many spanning trees is as follows:



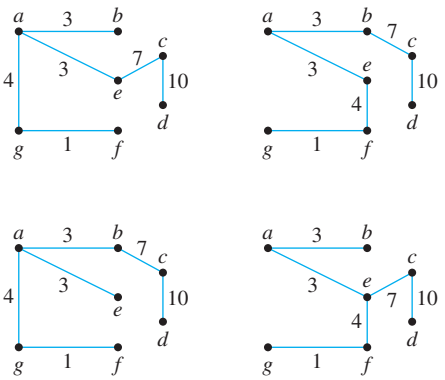
5. Minimum spanning tree:



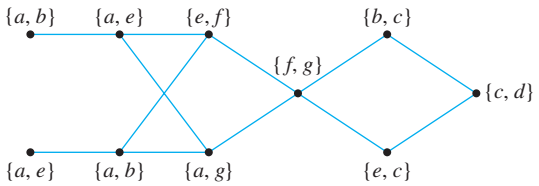
Order of adding the edges:
$\{a, b\}, \{e, f\}, \{e, d\}, \{d, c\}, \{g, f\}, \{b, c\}$

7. Minimum spanning tree: same as in exercise 5 Order of adding the edges:
$\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, g\}$

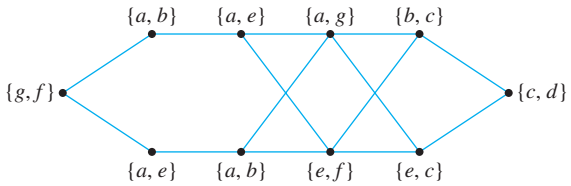
9. There are four minimum spanning trees:



When Prim's algorithm is used, edges are added in any of the orders obtained by following one of the eight paths from left to right across the diagram below.



When Kruskal's algorithm is used, edges are added in any of the orders obtained by following one of the eight paths from left to right across the diagram below.



12. Let N = Nashville, S = St. Louis, Lv = Louisville, Ch = Chicago, Cn = Cincinnati, D = Detroit, Mw = Milwaukee, and Mn = Minneapolis.

Step	$V(T)$	$E(T)$	F
0	$\{N\}$	$\varnothing$	$\{N\}$
1	$\{N\}$	$\varnothing$	$\{Lv, Mn\}$
2	$\{N, Lv\}$	$\{\{N, Lv\}\}$	$\{Mn, S, Cn, Ch, D, Mw\}$
3	$\{N, Lv, Cn\}$	$\{\{N, Lv\}, \{Lv, Cn\}\}$	$\{Mn, S, Ch, D, Mw\}$
4	$\{N, Lv, Cn, S\}$	$\{\{N, Lv\}, \{Lv, Cn\}, \{Lv, S\}\}$	$\{Mn, Ch, D, Mw\}$
5	$\{N, Lv, Cn, S, Ch\}$	$\{\{N, Lv\}, \{Lv, Cn\}, \{Lv, S\}, \{Lv, Ch\}\}$	$\{Mn, D, Mw\}$
6	$\{N, Lv, Cn, S, Ch, D\}$	$\{\{N, Lv\}, \{Lv, Cn\}, \{Lv, S\}, \{Lv, Ch\}\{Lv, D\}\}$	$\{Mn, Mw\}$
7	$\{N, Lv, Cn, S, Ch, D, Mw\}$	$\{\{N, Lv\}, \{Lv, Cn\}, \{Lv, S\}, \{Lv, Ch\}\{Lv, D\}, \{Ch, Mw\}\}$	$\{Mn\}$
8	$\{N, Lv, Cn, S, Ch, D, Mw, Mn\}$	$\{\{N, Lv\}, \{Lv, Cn\}, \{Lv, S\}, \{Lv, Ch\}, \{Lv, D\}, \{Ch, Mw\}, \{N, Mn\}\}$	

Step	$L(N)$	$L(S)$	$L(Lv)$	$L(Cn)$	$L(Ch)$	$L(D)$	$L(Mw)$	$L(Mn)$
0	**0**	∞	∞	∞	∞	∞	∞	∞
1	0	∞	**151**	∞	∞	∞	∞	695
2	0	393	151	**234**	420	457	499	695
3	0	**393**	151	234	420	457	499	695
4	0	393	151	234	**420**	457	499	695
5	0	393	151	234	420	**457**	494	695
6	0	393	151	234	420	457	**494**	695
7	0	393	151	234	420	457	494	**695**

Thus the shortest path from Nashville to Minneapolis has length $L(Mn) = 695$ miles.

In step 2 $D(Lv) = N$, in step 3 $D(Cn) = Lv$, in step 4 $D(S) = Cn$, in step 5 $D(Ch) = Lv$, in step 6 $D(D) = Lv$, in step 7 $D(Mw) = Ch$, and in step 8 $D(Mn) = N$. Tracing backwards from Mn gives $D(Mn) = N$, which is the starting point. So the shortest path is the direct route from Nashville to Minneapolis, without any intermediary stops.

13.

Step	$V(T)$	$E(T)$	F	$L(a)$	$L(b)$	$L(c)$	$L(d)$	$L(e)$	$L(z)$
0	$\{a\}$	$\varnothing$	$\{a\}$	**0**	∞	∞	∞	∞	∞
1	$\{a\}$	$\varnothing$	$\{b, d\}$	0	2	∞	**1**	∞	∞
2	$\{a, d\}$	$\{\{a, d\}\}$	$\{b, c, e\}$	0	**2**	6	1	11	∞
3	$\{a, b, d\}$	$\{\{a, d\}, \{a, b\}\}$	$\{c, e\}$	0	2	**5**	1	6	∞
4	$\{a, b, c, d\}$	$\{\{a, d\}, \{a, b\}, \{b, c\}\}$	$\{e, z\}$	0	2	5	1	**6**	13
5	$\{a, b, c, d, e\}$	$\{\{a, d\}, \{a, b\}, \{b, c\}, \{c, e\}\}$	$\{z\}$	0	2	5	1	6	**8**
6	$\{a, b, c, d, e, z\}$	$\{\{a, d\}, \{a, b\}, \{b, c\}, \{c, e\}, \{e, z\}\}$							

Thus the shortest path from a to z has length $L(z) = 8$.

In step 2 $D(d) = a$, in step 3 $D(b) = b$, in step 4 $D(c) = b$, in step 5 $D(e) = c$, and in step 6 $D(z) = e$. Tracing backwards from z gives $D(z) = e$, $D(e) = c$, $D(c) = b$, and $D(b) = a$. So the shortest path from a to z is $abcez$.

18. b. Proof: Suppose not. Suppose that for some tree T, u and v are distinct vertices of T, and P_1 and P_2 are two distinct paths joining u and v. *[We must deduce a contradiction. In fact, we will show that T contains a circuit.]* Let P_1 be denoted $u = v_0, v_1, v_2, \ldots, v_m = v$, and let P_2 be denoted $u = w_0, w_1, w_2, \ldots, w_n = v$. Because P_1 and P_2 are distinct, and T has no parallel edges, the sequence of vertices in P_1 must diverge from the sequence of vertices in P_2 at some point. Let i be the least integer such that $v_i \neq w_i$. Then $v_{i-1} = w_{i-1}$. Let j and k be the least integers greater than i so that $v_j = w_k$. (There must be such integers because $v_m = w_n = v$.) Then

$$v_{i-1}v_iv_{i+1}\ldots v_j(=w_k)w_{k-1}\ldots w_iw_{i-1}(=v_{i-1})$$

is a circuit in T. The existence of such a circuit contradicts the fact that T is a tree. Hence the supposition must be false. That is, given any tree with vertices u and v, there is a unique path joining u and w.

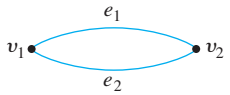
20. Proof: Suppose G is a connected graph, T is a circuit-free subgraph of G, and if any edge e of G not in T is added to T, the resulting graph contains a circuit. Suppose that T is not a spanning tree for G. *[We must derive a contradiction.]*

Case 1 (T is not connected): In this case, there are vertices u and v in T such that there is no walk in T from u to v. Now, since G is connected, there is a walk in G from u to v, and hence, by Lemma 10.2.1, there is a path in G from u to v. Let $e_1, e_2, \ldots, e_k$ be the edges of this path that are not in T. When these edges are added to T, the result is a graph T' in which u and v are connected by a path. In addition, by hypothesis, each of the edges e_i creates a circuit when added to T. Now remove these edges one by one from T'. By the same argument used in the proof of Lemma 10.5.3, each such removal leaves u and v connected since each e_i is an edge of a circuit when added to T. Hence, after all the e_i have been removed, u and v remain connected. But this contradicts the fact that there is no walk in T from u to v.

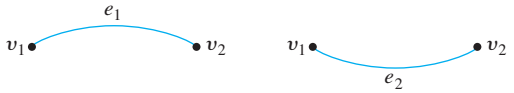
Case 2 (T is connected): In this case, since T is not a spanning tree and T is circuit-free, there is a vertex v in G such that v is not in T. *[For if T were connected, circuit-free, and contained every vertex in G, then T would be a spanning tree for G.]* Since G is connected, v is not isolated. Thus there is an edge e in G with v as an endpoint. Let T' be the graph obtained from T by adding e and v. *[Note that e is not already in T because if it were, its endpoint v would also be in T and it is not.]* Then T' contains a circuit because, by hypothesis, addition of any edge to T creates a circuit. Also T' is connected because T is and because when e is added to T, e becomes part of a circuit in T'. Now deletion of an edge from a circuit does not disconnect a graph, so if e is deleted from T' the result is a connected graph. But the resulting graph contains v, which means that there is an edge in T connecting v to another vertex of T. This implies that v is in T *[because both endpoints of any edge in a graph must be part of the vertex set of the graph]*, which contradicts the fact that v is not in T.

Thus, in either case, the supposition that T is not a spanning tree leads to a contradiction. Hence the supposition is false, and T is a spanning tree for G.

21. a. No. Counterexample: Let G be the following graph.



Then G has the spanning trees shown below.



22. *Hint*: Suppose e is contained in every spanning tree of G and the graph obtained by removing e from G is connected. Let G' be the subgraph of G obtained by removing e, and let T' be a spanning tree for G'. How is T' related to G?

24. Proof: Suppose that $w(e') > w(e)$. Form a new graph T' by adding e to T and deleting e'. By exercise 20, addng an edge to a spanning tree creates a circuit, and by Lemma 10.5.3, deleting an edge from a circuit does not disconnect a graph. Consequently, T' is also a spanning tree for G. Furthermore, $w(T') < w(T)$ because $w(T') = w(T) - w(e') + w(e) = w(T) - (w(e') - w(e)) < w(T)$ *[since $w(e') > w(e)$, which implies that $w(e') - w(e) > 0$]*. But this contradicts the fact that T is a minimum spanning tree for G. Hence the supposition is false, and so $w(e') \leq w(e)$.

25. *Hint:* Suppose e is an edge that has smaller weight than any other edge of G, and suppose T is a minimum spanning tree for G that does not contain e. Create a new spanning tree T' by adding e to T and removing another edge of T (which one?). Then $w(T') < w(T)$.

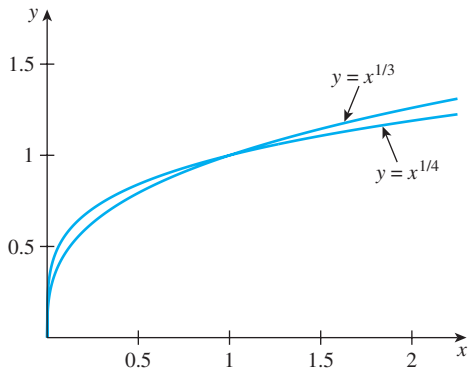
26. Yes. Proof by contradiction: Suppose G is a weighted graph in which all the weights of all the edges are distinct, and suppose G has two distinct minimum spanning trees T_1 and T_2. Let e be the edge of least weight that is in one of the trees but not the other. Without loss of generality, we may say that e is in T_1. Add e to T_2 to obtain a graph G'. By exercise 19, G' contains a nontrivial circuit. At least one other edge f of this circuit is not in T_1 because otherwise T_1 would contain the complete circuit, which would contradict the fact that T_1 is a tree. Now f has weight greater than e because all edges have distinct weights, f is in T_2 and not in T_1, and e is the edge of least weight that is in one of the trees and not the other. Remove f from G' to obtain a tree T_3. Then $w(T_3) < w(T_2)$ because T_3 is the same as T_2 except that it contains e rather than f and $w(e) < w(f)$. Consequently, T_3 is a spanning tree for G of smaller weight than T_2. This contradicts the supposition that T_2 is a minimum spanning tree for G. Thus G cannot have more than one minimum spanning tree.

28. The output will be a "minimum spanning forest" for the graph. It will contain a minimum spanning tree for each connected component of the input graph.

SECTION 11.1

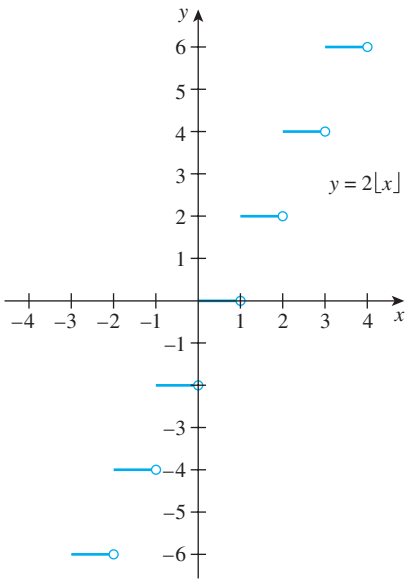
1. **a.** $f(0)$ is positive.
b. $f(x) = 0$ when $x = -2$ and $x = 3$ (approximately)
c. $x_1 = -1$ and $x_2 = 2$ (approximately)
d. $x = 1$ or $x = -\frac{1}{2}$ (approximately)
e. increase
f. decrease

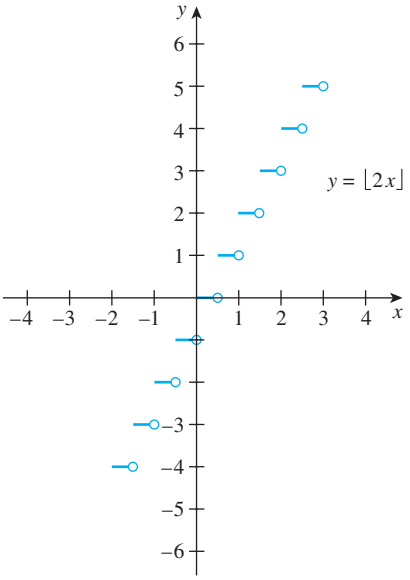
3.



When $0 < x < 1$, $x^{1/3} < x^{1/4}$. When $x > 1$, $x^{1/3} > x^{1/4}$.

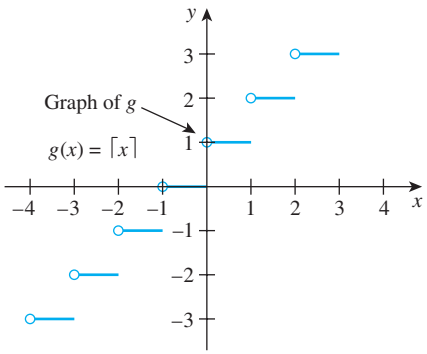
5.





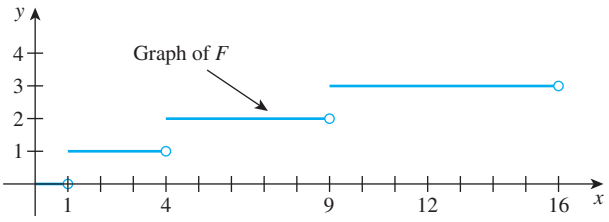
The graphs show that $2\lfloor x \rfloor \neq \lfloor 2x \rfloor$ for many values of x.

6.



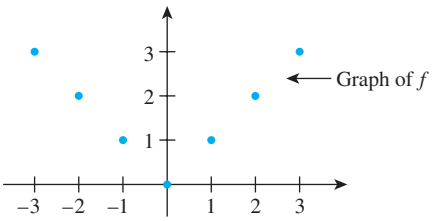
8.

x	$F(x) = \lfloor x^{1/2} \rfloor$
0	0
$\frac{1}{2}$	0
1	1
2	1
3	1
4	2



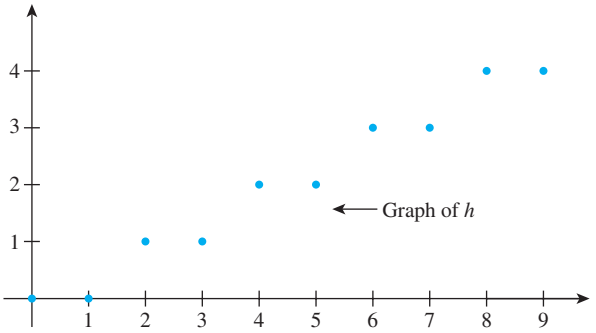
10.

n	$f(n) = \lvert n \rvert$
0	0
1	1
2	2
3	3
−1	1
−2	2
−3	3



12.

n	$h(n) = \left\lfloor \frac{n}{2} \right\rfloor$
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3
8	4
9	4



14. f is increasing on the intervals $\{x \in \mathbf{R} \mid -3 < x < -2\}$ and $\{x \in \mathbf{R} \mid 0 < x < 2.5\}$, and f is decreasing on $\{x \in \mathbf{R} \mid -2 < x < 0\}$ and $\{x \in \mathbf{R} \mid 2.5 < x < 4\}$ (approximately).

15. Proof: Suppose that x_1 and x_2 are particular but arbitrarily chosen real numbers such that $x_1 < x_2$. *[We must show that $f(x_1) < f(x_2)$.]* Since

$$x_1 < x_2$$

then

$$2x_1 < 2x_2$$

and

$$2x_1 - 3 < 2x_2 - 3$$

by basic properties of inequalities. Thus, by definition of f,

$$f(x_1) < f(x_2)$$

[as was to be shown]. Hence f is increasing on the set of all real numbers.

17. a. Proof: Suppose x_1 and x_2 are real numbers with $x_1 < x_2 < 0$. *[We must show that $h(x_1) > h(x_2)$.]* Multiply both sides of $x_1 < x_2$ by x_1 to obtain $(x_1)^2 > x_1x_2$ *[by T23 of Appendix A since $x_1 < 0$]*, and multiply both sides of $x_1 < x_2$ by x_2 to obtain $x_1x_2 > (x_2)^2$ *[by T23 of Appendix A since $x_2 < 0$].* By transitivity of order *[Appendix A, T18]* $(x_2)^2 < (x_1)^2$, and so, by definition of h, $h(x_2) < h(x_1)$.

18. a. *Preliminaries:* If both x_1 and x_2 are positive, then by the rules for working with inequalities (see Appendix A),

$$\frac{x_1 - 1}{x_1} < \frac{x_2 - 1}{x_2} \Rightarrow x_2(x_1 - 1) < x_1(x_2 - 1)$$

by multiplying both sides by x_1x_2 (which is positive)

$$\Rightarrow x_1x_2 - x_2 < x_1x_2 - x_1$$

by multiplying out

$$\Rightarrow -x_2 < -x_1$$

by subtracting x_1x_2 from both sides

$$\Rightarrow x_2 > x_1$$

by multiplying by -1.

Are these steps reversible? Yes!

Proof: Suppose that x_1 and x_2 are positive real numbers and $x_1 < x_2$. *[We must show that $k(x_1) < k(x_2)$.]* Then

$x_1 < x_2$

$\Rightarrow -x_2 < -x_1$ by multiplying by -1

$\Rightarrow x_1x_2 - x_2 < x_1x_2 - x_1$ by adding x_1x_2 to both sides

$\Rightarrow x_2(x_1 - 1) < x_1(x_2 - 1)$ by factoring both sides

$\Rightarrow \dfrac{x_1 - 1}{x_1} < \dfrac{x_2 - 1}{x_2}$ by dividing both sides by the positive number x_1x_2

$\Rightarrow k(x_1) < k(x_2)$ by definition of k.

[This is what was to be shown.]

19. Proof: Suppose f: $\mathbf{R} \to \mathbf{R}$ is increasing. *[We must show that f is one-to-one. In other words, we must show that for all real numbers x_1 and x_2, if $x_1 \neq x_2$ then $f(x_1) = f(x_2)$.]* Suppose x_1 and x_2 are real numbers and $x_1 \neq x_2$. By the trichotomy law *[Appendix A, T17]* $x_1 < x_2$, or $x_1 > x_2$. In case $x_1 < x_2$, then since f is increasing, $f(x_1) < f(x_2)$ and so $f(x_1) \neq f(x_2)$. Similarly, in case $x_1 > x_2$, then $f(x_1) > f(x_2)$ and so $f(x_1) \neq f(x_2)$. Thus in either case, $f(x_1) \neq f(x_2)$ *[as was to be shown]*.

21. a. Proof: Suppose u and v are nonnegative real numbers with $u < v$. *[We must show that $f(u) < f(v)$.]* Note that $v = u + h$ for some positive real number h. By substitution and the binomial theorem,

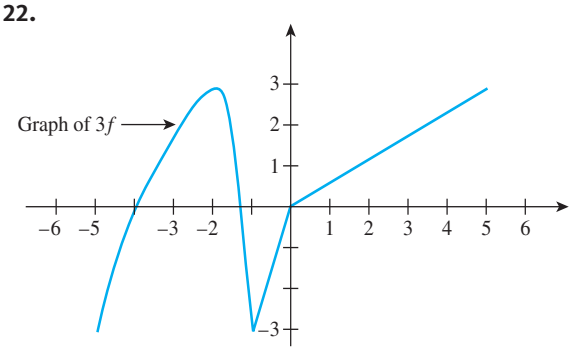
$$v^m = (u+h)^m = u^m + \left[\binom{m}{1}u^{m-1}h + \binom{m}{2}u^{m-2}h^2 + \cdots + \binom{m}{m-1}uh^{m-1} + h^m\right].$$

The bracketed sum is positive because $u \geq 0$ and $h > 0$, and a sum of nonnegative terms that includes at least one positive term is positive. Hence

$$v^m = u^m + \text{a positive number},$$

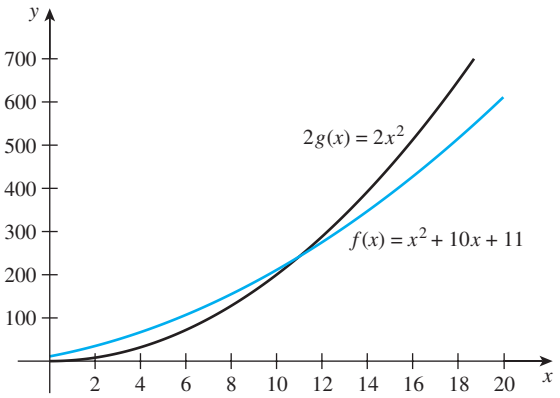
and so $f(u) = u^m < v^m = f(v)$ *[as was to be shown]*.

22.



24. Proof: Suppose that f is a real-valued function of a real variable, f is decreasing on a set S, and M is any positive real number. *[We must show that Mf is decreasing on S. In other words, we must show that for all x_1 and x_2 in S, if $x_1 < x_2$ then $(Mf)(x_1) > (Mf)(x_2)$.]* Suppose x_1 and x_2 are in S and $x_1 < x_2$. Since f is decreasing on S, $f(x_1) > f(x_2)$, and since M is positive, $Mf(x_1) > Mf(x_2)$ *[because when both sides of an inequality are multiplied by a positive number, the direction of the inequality is unchanged]*. It follows by definition of Mf that $(Mf)(x_1) > (Mf)(x_2)$ *[as was to be shown]*.

27. To find the answer algebraically, solve the equation $2x^2 = x^2 + 10x + 11$ for x. Subtracting x^2 from both sides gives $x^2 - 10x - 11 = 0$, and either using the quadratic formula or factoring $x^2 - 10x - 11 = (x - 11)(x + 1)$ gives $x = 11$ (since $x > 0$). To find an approximate answer with a graphing calculator, plot both $f(x) = x^2 + 10x + 11$ and $2g(x) = 2x^2$ for $x > 0$, as shown in the figure, and find that $2g(x) > f(x)$ when $x > 11$ (approximately). You can obtain only an approximate answer from a graphing calculator because the calculator computes values only to an accuracy of a finite number of decimal places.



SECTION 11.2

1. a. *Formal version of negation:* $f(n)$ is not $\Omega(g(n))$ if, and only if, $\forall$ positive real numbers a and A, $\exists$ an integer $n \geq a$ such that $Ag(n) > f(n)$.

b. *Informal version of negation:* $f(n)$ is not $\Omega(g(n))$ if, and only if, no matter what positive real numbers a and A might be chosen, it is possible to find an integer n greater than or equal to a with the property that $Ag(n) > f(n)$.

4. $n - \left\lfloor \dfrac{n}{2} \right\rfloor + 1$ is $\Omega(n)$

5. $n - \left\lfloor \dfrac{n}{2} \right\rfloor + 1$ is $O(n)$

6. $3n(n-2)$ is $\Theta(n^2)$

10. a. For each integer $n \geq 1$,

$$0 \leq 2n^2 + 15n + 4$$

because all terms in $2n^2 + 15n + 4$ are positive. Moreover,

$$2n^2 + 15n + 4 \le 2n^2 + 15n^2 + 4n^2$$
because when $n \ge 1$, $15n \le 15n^2$ and $4 \le 4n^2$
$$= 21n^2$$ by combining like terms.

Therefore, by transitivity of equality and order,

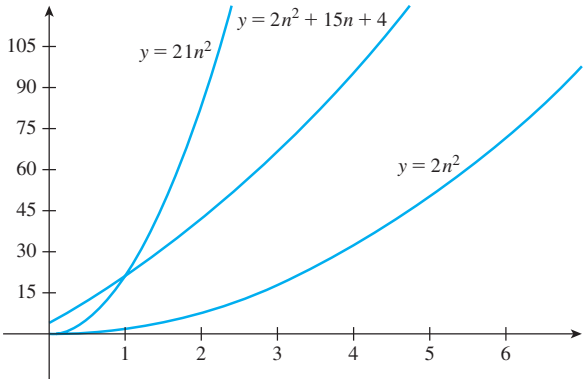
$$0 \le 2n^2 + 15n + 4 \le 21n^2 \quad \text{for each integer } n \ge 1.$$

b. For each integer $n \ge 1$,

$$2n^2 \le 2n^2 + 15n + 4$$

because $15n + 4 > 0$ since n is positive.

c. Sketch of graph



d. Let $A = 2$ and $a = 1$. Then, by substitution from the result of part (b),

$$An^2 < 2n^2 + 15n + 4 \quad \text{for each integer } n \ge a,$$

and hence, by definition of Ω-notation, $2n^2 + 15n + 4$ is $\Omega(n^2)$. Let $B = 21$ and $6 = 1$. Then, by substitution from the result of part (a),

$$0 < 2n^2 + 15n + 4 \le Bn^2 \quad \text{for each integer } n \ge 6,$$

and hence by definition of O-notation, $2n^2 + 15n + 4$ is $O(n^2)$.

e. *Solution 1:* Let $A = 2$, $B = 21$, and $k = 1$. By the results of parts (a) and (b),

$$An^2 \le 2n^2 + 15n + 4 \le Bn^2 \quad \text{for each integer } n \ge k,$$

and hence, by definition of Θ-notation, $2n^2 + 15n + 4$ is $\Theta(n^2)$.

Solution 2: By part (d), $2n^2 + 15n + 4$ is both $\Omega(n^2)$ and $O(n^2)$. Hence, by Theorem 11.2.1,

$$2n^2 + 15n + 4 \text{ is } \Theta(n^2).$$

13. For each integer $n \ge 1$,

$$5n^3 \le 5n^3 + 65n + 30$$

because $65n + 30 > 0$ since n is positive. Moreover,

$$5n^3 + 65n + 30 \le 5n^3 + 65n^3 + 30n^3$$
because when $n \ge 1$, then $65n < 65n^3$ and $30 < 30n^3$
$$= 100n^3$$ by combining like terms.

Therefore, by transitivity of order and equality,

$$5n^3 \le 5n^3 + 65n + 30 \le 100n^3.$$

Thus, let $A = 5$, $B = 100$, and $k = 1$. Then

$$An^3 \le 5n^3 + 65n + 30 \le Bn^3 \quad \text{for each integer } n \ge k,$$

and hence, by definition of Θ-notation, $5n^3 + 65n + 30$ is $\Theta(n^3)$.

15. For each integer $n \ge 1$,

$$n \le n + \frac{1}{2} < n + 1,$$

and so $\lfloor n + \frac{1}{2} \rfloor = n$, by definition of floor, and $\lfloor n + \frac{1}{2} \rfloor$ is nonnegative. In addition, when $n \ge 1$, then $n + 1 \le n + n = 2n$, and thus, by transitivity of equality and order,

$$n \le \left\lfloor n + \frac{1}{2} \right\rfloor \le 2n.$$

Let $A = 1$, $B = 2$, and $k = 1$. Then

$$An \le \left\lfloor n + \frac{1}{2} \right\rfloor \le Bn \quad \text{for every integer } n \ge k,$$

and hence, by definition of Θ-notation, $\lfloor n + \frac{1}{2} \rfloor$ is $\Theta(n)$.

18. Proof of Theorem 11.2.7(b):
Suppose f and g are real-valued functions defined on the same set of nonnegative integers, suppose $f(n) \ge 0$ and $g(n) \ge 0$ for every integer $n \ge r$, where r is a positive real number, and suppose $f(n)$ is $\Theta(g(n))$. *[We must show that $g(n)$ is $\Theta(f(n)$.]* By definition of Θ-notation, there exist positive real numbers A, B, and k with $k \ge r$ such that for each integer $n \ge k$,

$$Ag(n) \le f(n) \le Bg(n).$$

Dividing the left-hand inequality by A and the right-hand inequality by B gives that

$$g(n) \le \frac{1}{A} f(n) \quad \text{and} \quad \frac{1}{B} f(n) \le g(n),$$

and combining the resulting inequalities produces

$$\frac{1}{B} f(n) \le g(n) \le \frac{1}{A} f(n) \quad \text{for each integer } n \ge k.$$

Now both $f(n) \ge 0$ and $g(n) \ge 0$ for each integer $n \ge k$. Also, since both A and B are positive real numbers, so are $1/A$ and $1/B$. Thus, by definition of Θ-notation, $g(n)$ is $\Theta(f(n))$.

20. Proof (by contradiction): Suppose not. That is, suppose n^5 is $O(n^2)$. *[We must show that this supposition leads to a contradiction.]* By definition of O-notation, there exist positive real numbers B and b such that

$$0 \le n^5 \le Bn^2 \quad \text{for each integer } n \ge b.$$

Dividing the inequalities by n^2 and taking the cube root of both sides gives

$$0 \le n \le \sqrt[3]{B} \quad \text{for each integer } n \ge b.$$

These two conditions are contradictory because on the one hand n can be any integer greater than or equal to b, but when n is greater than b, then n is less than $\sqrt[3]{B}$, which is a fixed integer. Thus the supposition leads to a contradiction, and hence the supposition is false.

22. a. *Solution 1 (using ad hoc calculations):* Let $\Leftrightarrow$ stand for the words "if, and only if," and observe that

$$(*) \qquad \frac{1}{2}n^4 \le 2n^4 - 90n^3 + 3$$

$$\Leftrightarrow \quad n^4 \le 4n^4 - 180n^3 + 6$$

because dividing or multiplying both sides of an inequality by 2, which is positive, preserves the direction of the inequality.

$$\Leftrightarrow \quad 180n^3 - 6 \le 3n^4$$

because adding or subtracting $180n^3 - 6$ to both sides of an inequality preserves the direction of the inequality.

$$(**) \Leftrightarrow \quad 60 - \frac{2}{n^3} \le n$$

because dividing or multiplying both sides of an inequality by $3n^3$, which is positive, preserves the direction of the inequality.

Because all the inequalities are equivalent (that is, each inequality is true if, and only if, all the others are true), any value of n that makes inequality (**) true makes inequality (*) true also. Now

$$\text{if} \quad n \ge 60, \quad \text{then} \quad n \ge 60 - \frac{2}{n^3},$$

which is inequality (**). Therefore, inequality (*) is also true for $n \ge 60$, for every integer $n \ge 60$,

$$\frac{1}{2}n^4 \le 2n^4 - 90n^3 + 3.$$

Let $A = \frac{1}{2}$ and $a = 60$. Then for every integer $n \ge a$,

$$An^4 \le 2n^4 - 90n^3 + 3.$$

and so, by definition of Ω-notation, $2n^4 - 90n^3 + 3$ is $\Omega(n^4)$.

Solution 2 (using the general procedure):
To use the general procedure from Example 11.2.4 to show that $2n^4 - 90n^3 + 3$ is $\Omega(n^4)$, let

$$A = \frac{1}{2} \cdot 2 = 1 \quad \text{and} \quad a = \frac{2}{2}(|-90| + |3|) = 93$$

and note that $a \ge 1$. We will show that $n^4 \le 2n^4 - 90n^3 + 3$ for every integer $n \ge a$. Now $n \ge a$ means that

$$n \ge 90 + 3.$$

Multiplying both sides by n^3 gives

$$n^4 \ge 90n^3 + 3n^3$$

and subtracting first $3n^3$ and then 3 from the right-hand side gives that

$$n^4 \ge 90n^3 \ge 90n^3 - 3 \quad \text{for every integer } n \ge a.$$

Subtracting the right-hand side from the left-hand side and adding n^4 to both sides gives

$$2n^4 - 90n^3 + 3 \ge n^4 \quad \text{for every integer } n \ge a.$$

Thus since $A = 1$,

$$2n^4 - 90n^3 + 3 \ge An^4 \quad \text{for every integer } n \ge a,$$

and so, by definition of Ω-notation, $2n^4 - 90n^3 + 3$ is $\Omega(n^4)$.

b. To show that $2n^4 - 90n^3 + 3$ is $O(n^4)$, observe that for every integer $n \ge 1$,

$$2n^4 - 90n^3 + 3 \le 2n^4 + 90n^3 + 3$$

because when $n \ge 1$, then $90n^3$ is positive

$$\le 2n^4 + 90n^4 + 3n^4$$

by Theorem 11.2.2 (since $n \ge 1$, $n^3 \le n^4$ and $1 \le n^4$, and so $90n^3 \le 90n^4$ and $3 \le 3n^4$)

$$= 95n^4$$

because $2 + 90 + 3 = 95$.

Thus, by transitivity of order and equality, for every integer $n \ge 1$,

$$2n^4 - 90n^3 + 3 \le 95n^4.$$

In addition, by part (a), for every integer $n \ge 60$,

$$\frac{1}{2}n^4 \le 2n^4 - 90n^3 + 3$$

so since $0 \le \frac{1}{2}n^4$, transitivity of order gives that for every integer $n \ge 60$,

$$0 \le 2n^4 - 90n^3 + 3 \le 95n^4.$$

Let $B = 14$ and $b = 60$. Then, for every integer $n \ge b$,

$$0 \le 2n^4 - 90n^3 + 3 \le Bn^4$$

and hence, by definition of O-notation,

$$2n^4 - 90n^3 + 3 \text{ is } O(n^4).$$

c. *Solution 1:* Let $A = \frac{1}{2}$, $B = 95$, and $k = 60$. By the results of parts (a) and (b), for every integer $n \ge k$,

$$An^4 \le 2n^4 - 90n^3 + 3 \le Bn^4$$

and hence, by definition of Θ-notation,

$$2n^4 - 90n^3 + 3 \text{ is } \Theta(n^4).$$

Solution 2: By parts (a) and (b), $2n^4 - 90n^3 + 3$ is both $\Omega(n^4)$ and $O(n^4)$. Hence, by Theorem 11.2.1,

$$2n^4 - 90n^3 + 3 \text{ is } \Theta(n^4).$$

25. Proof: Suppose

$$P(n) = a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0$$

where all the coefficients $a_0, a_1, \ldots, a_m$ are real numbers and $a_m > 0$.

a. ***Proof that P(n) is $\Omega(n^m)$:*** According to the general procedure described in Example 11.2.4, we let

$$A = \frac{1}{2}a_m,$$

$$d = 2\left(\frac{|a_{m-1}| + |a_{m-2}| + \cdots + |a_2| + |a_1| + |a_0|}{a_m}\right),$$

and $a = \max(d, 1)$.

Then $n \geq a$ means that

$$n \geq 2\left(\frac{|a_{m-1}| + |a_{m-2}| + \cdots + |a_2| + |a_1| + |a_0|}{a_m}\right).$$

Multiplying both sides by $\frac{1}{2}a_m n^{m-1}$ gives

$$\begin{aligned}\frac{1}{2}a_m n^m &\geq (|a_{m-1}| + |a_{m-2}| + \cdots + |a_2| + |a_1| + |a_0|)n^{m-1} \\ &= |a_{m-1}|n^{m-1} + |a_{m-2}|n^{m-1} + \cdots \\ &\qquad + |a_2|n^{m-1} + |a_1|n^{m-1} + |a_0|n^{m-1} \\ &\geq |a_{m-1}|n^{m-1} + |a_{m-2}|n^{m-2} + \cdots + |a_2|n^2 + |a_1|n + |a_0|\end{aligned}$$

because $n^{m-1} \geq n^r$ for each $r \leq m-1$ since $n \geq 1$.

Thus, by transitivity of order and equality, for each integer $n \geq a$,

$$\left(\frac{a_m}{2}\right)n^m \geq |a_{m-1}|n^{m-1} + |a_{m-2}|n^{m-1} + \cdots + |a_1|n + |a_0|.$$

Subtracting the right side from the left gives

$$\left(\frac{a_m}{2}\right)n^m - |a_{m-1}|n^{m-1} - |a_{m-2}|n^{m-1} - \cdots - |a_1|n - |a_0| \geq 0$$

for each integer $n \geq a$. It follows that, for each integer $n \geq a$,

$$\left(\frac{a_m}{2}\right)n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0 \geq 0$$

because, by definition of absolute value, each $-|a_i| \leq a_i$. Adding $\left(\frac{a_m}{2}\right)n^m$ to both sides gives that, for each integer $n \geq a$,

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0 \geq \left(\frac{a_m}{2}\right)n^m$$

Therefore, with $A = \frac{a_m}{2}$ and $a = \max(d, 1)$, we have that for each integer $n \geq a$,

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0 \geq An^m,$$

and so, by definition of Ω-notation,

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0$$

is $\Omega(n^m)$.

b. ***Proof that P(n) is $O(n^m)$:*** Observe that for each integer $n \geq 1$,

$$\begin{aligned}&a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0 \\ &\quad \leq |a_m|n^m + |a_{m-1}|n^{m-1} + |a_{m-2}|n^{m-2} \\ &\qquad + \cdots + |a_2|n^2 + |a_1|n + |a_0|\end{aligned}$$

because by definition of absolute value each $a_i \leq |a_i|$

$$\begin{aligned}&\quad \leq |a_m|n^m + |a_{m-1}|n^m + |a_{m-2}|n^m \\ &\qquad + \cdots + |a_2|n^m + |a_1|n^m + |a_0|n^m\end{aligned}$$

by Theorem 11.2.2 since $n \geq 1$, $n^{m-i} \leq n^m$ for each i from 0 through m

$$= (|a_m| + |a_{m-1}| + |a_{m-2}| + \cdots + |a_2| + |a_1| + |a_0|)n^m$$

Let

$$B = |a_m| + |a_{m=1}| + |a_{m=2}| + \cdots + |a_2| + |a_1| + |a_0|.$$

Then, by transitivity of order and equality, for each integer $n \geq 1$,

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0 \leq Bn^m.$$

In addition, by part (a), there exists a positive real number a such that for each integer $n \geq a$,

$$\frac{a_m}{2}n^m \leq a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0.$$

Now $\frac{a_m}{2}n^m > 0$ because $a_m > 0$, and thus, transitivity of order gives that for each integer $n \geq a$,

$$0 \leq a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0$$

Let $b = \max(1, a)$. Then, for each integer $n \geq b$,

$$0 \leq a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0 \leq Bn^m,$$

and hence, by definition of O-notation,

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0$$

is $O(n^m)$.

c. ***Proof that P(n) is $\Theta(n^m)$:*** By parts (a) and (b),

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0$$

is both $\Omega(n^m)$ and $O(n^m)$. Hence, by Theorem 11.2.1,

$$a_m n^m + a_{m-1}n^{m-1} + a_{m-2}n^{m-2} + \cdots + a_1 n + a_0$$

is $\Theta(n^m)$.

26. $$\begin{aligned}\frac{(n+1)(n-2)}{4} &= \frac{1}{4}(n^2 + n - 2n - 2) = \frac{1}{4}(n^2 - n - 2) \\ &= \frac{1}{4}n^2 - \frac{1}{4}n - \frac{1}{2},\end{aligned}$$

which is $\Theta(n^2)$ by the theorem on polynomial orders.

29. $$\begin{aligned}\frac{n(n+1)(2n+1)}{6} &= \frac{1}{6}[n(n+1)(2n+1)] \\ &= \frac{1}{6}[(n^2+n)(2n+1)] \\ &= \frac{1}{6}(2n^3 + 3n^2 + n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n,\end{aligned}$$

which is $\Theta(n^3)$ by the theorem on polynomial orders.

32. By exercise 10 of Section 5.2, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, which is $\Theta(n^3)$ by exercise 29 above. Hence $1^2 + 2^2 + 3^2 + \cdots + n^2$ is $\Theta(n^3)$.

34. Note that

$$\begin{aligned}2 + 4 + 6 + \cdots + 2n &= 2(1 + 2 + 3 + \cdots + n) && \text{by factoring out a 2} \\ &= 2\left(\frac{n(n+1)}{2}\right) && \text{by Theorem 5.2.1} \\ &= n^2 + n && \text{by algebra,}\end{aligned}$$

and so, by the theorem on polynomial orders,

$$2 + 4 + 6 + \cdots + 2n \text{ is } \Theta(n^2).$$

36. Note that

$$\begin{aligned}\sum_{i=1}^{n}(4i-9) &= 4\sum_{i=1}^{n} i - \sum_{i=1}^{n} 9 && \text{by Theorem 5.1.1}\\ &= 4\left(\frac{n(n+1)}{2}\right) - (\underbrace{9+9+\cdots+9}_{n \text{ terms}}) && \text{by Theorem 5.2.1}\\ &= 2n^2+2n-9n && \text{by definition of mutiplication}\\ &= 2n^2-7n && \text{by algebra,}\end{aligned}$$

and so, by the theorem on polynomial orders,

$$\sum_{i=1}^{n}(4i-9) \quad \text{is} \quad \Theta(n^2).$$

38. *Hint:* Use the result of exercise 13 from Section 5.2.

40. a. Proof: Suppose c is a positive real number and f is a real-valued function defined on a set of nonnegative integers with $f(n) \geq 0$ for each integer n greater than or equal to a positive real number k. Now if we let $A = B = c$, we have that for each integer $n \geq k$,

$$Af(n) \leq cf(n) \leq Bf(n)$$

and so, by definition of Θ-notation, $cf(n)$ is $\Theta(f(n))$.

b. Let $c = 3$ and $f(n) = n$. Then f is a real-valued function and $f(n) \geq 0$ for each integer $n \geq 0$. So by part (a), $cf(n)$ is $\Theta(f(n))$, or, by substitution, $3n$ is $\Theta(n)$.

43. By exercise 15, $\left\lfloor \frac{n+1}{2} \right\rfloor$ is $\Theta(n)$, and by exercise 40(b), $3n$ is also $\Theta(n)$. Thus $\left\lfloor \frac{n+1}{2} \right\rfloor + 3n$ is $\Theta(n)$ by Theorem 11.2.9(a).

44. By exercise 28, $\frac{n(n-1)}{2}$ is $\Theta(n^2)$, by exercise 17, $\left\lfloor \frac{n}{2} \right\rfloor$ is $\Theta(n)$, and by exercise 41 (with $f(n) = 1$), 1 is $\Theta(1)$. Now $n \leq n^2$ and $1 \leq n^2$ for each integer $n \geq 1$. Thus $\frac{n(n-1)}{2} + \left\lfloor \frac{n}{2} \right\rfloor + 1$ is $\Theta(n^2)$ by Theorem 11.2.9(c).

46. a. Proof (by mathematical induction): Let the property $P(m)$ be the sentence

If n is any integer with $n > 1$, then $n^m > 1$. ←$P(m)$

Show that P(1) is true: We must show that if n is any integer with $n > 1$, then $n^1 > 1$. But this is true because $n^1 = n$. So $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is true: Let k be a particular but arbitrarily chosen integer with $k \geq 1$, and suppose that

If n is any integer with $n > 1$, then $n^k > 1$. ← $P(k)$ inductive hypothesis

We must show that

If n is any integer with $n > 1$, then $n^{k+1} > 1$. ←$P(k+1)$

So suppose n is any integer with $n > 1$. By inductive hypothesis, $n^k > 1$, and multiplying both sides by the positive number n gives $n \cdot n^k > n \cdot 1$, or, equivalently, $n^{k+1} > n$. Thus $n^{k+1} > n$ and $n > 1$, and so, by transitivity of order, $n^{k+1} > 1$ *[as was to be shown].*

b. Proof: Suppose n is any integer with $n > 1$ and r and s are integers with $r < s$. Then $s - r$ is an integer with $s - r \geq 1$, and so, by part (a), $n^{s-r} > 1$. Multiplying both sides by n^r gives $n^r \cdot n^{s-r} > n^r \cdot 1$, and so, by the laws of exponents, $n^s > n^r$ *[as was to be shown].*

47. a. Proof (by mathematical induction): Let the property $P(m)$ be the sentence

If $0 < x \leq 1$, then $x^m \leq 1$. ←$P(m)$

Show that P(1) is true: We must show that if $0 < x \leq 1$, then $x^1 \leq 1$. But $x \leq 1$ by assumption and $x^1 = x$. So $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true then P(k + 1) is true: Let k be any integer with $k \geq 1$, and suppose that

If $0 < x \leq 1$, then $x^k \leq 1$. ← $P(k)$ inductive hypothesis

We must show that

If $0 < x \leq 1$, then $x^{k+1} \leq 1$. ← $P(k+1)$

So let x be any number with $0 < x \leq 1$. By inductive hypothesis, $x^k \leq 1$, and multiplying both sides of this inequality by the nonnegative number x gives $x \cdot x^k \leq x \cdot 1$. Thus, by the laws of exponents, $x^{k+1} \leq x$. Then

$$x^{k+1} \leq x \text{ and } x \leq 1,$$

and hence, by the transitive property of order (T18 in Appendix A), $x^{k+1} \leq 1$.

b. *Hint:* What is the contrapositive of the statement in part (a)?

48. Proof of Theorem 11.2.6(b):
Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for each integer $n \geq r$. Suppose also that $g(n)$ is $O(f(n))$. We will show that $f(n)$ is $\Omega(g(n))$. By definition of O-notation, there are positive real numbers B and b such that $b \geq r$, and, for each integer $n \geq b$,

$$0 \leq g(n) \leq Bf(n)$$

Divide the right-hand inequality by B to obtain

$$\frac{1}{B}g(n) \leq f(n),$$

for each integer $n \geq b$. Let $A = 1/B$ and $a = b$. Then for each integer $n \geq a$,

$$Ag(n) \leq f(n)$$

and so $f(n)$ is $\Omega(g(n))$ by definition of Ω-notation.

50. a. Proof of Theorem 11.2.8(a):
Let f and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f(n) \geq 0$ and $g(n) \geq 0$ for each $n \geq r$. Suppose also that $f(n)$ is $\Omega(g(n))$ and c is any positive real number. *[We will show that $cf(n)$ is $\Omega(g(n))$.]* By definition of Ω-notation, there are positive real numbers A and a such that $a \geq r$, and, for each integer $n \geq a$,

$$Ag(n) \leq f(n).$$

Multiply both sides of the inequality by c to obtain

$$cAg(n) \leq cf(n),$$

and let $A' = Ac$. Then A' is a positive real number because both A and c are positive real numbers.

Hence there are positive real numbers A' and a such that $a \geq r$, and, for each integer $n \geq a$,

$$A'g(n) \leq cf(n).$$

Thus $cf(n)$ is $\Omega(g(n))$ by definition of Ω-notation.

51. a. Partial proof of Theorem 11.2.9(a): Let f_1, f_2, and g be real-valued functions defined on the same set of nonnegative integers, and suppose there is a positive real number r such that $f_1(n) \geq 0$, $f_2(n) \geq 0$, and $g(n) \geq 0$ for each integer $n \geq r$. Suppose also that $f_1(n)$ is $\Theta(g(n))$ and $f_2(n)$ is $\Theta(g(n))$. *[We will show that $(f_1(n) + f_2(n))$ is $\Theta(g(n))$.]* By definition of Θ-notation, there are positive real numbers A, B, A', B', k, and k' such that $k \geq r$, $k' \geq r$ and, for each integer n such that $n \geq k$ and $n \geq k'$,

$$Ag(n) \leq f_1(n) \leq Bg(n)$$

and

$$A'g(n) \leq f_2(n) \leq B'g(n).$$

Let $k'' = \max(k, k')$.

SECTION 11.3

1. a. $\log_2(200) = \frac{\ln 200}{\ln 2} \cong 7.6$ nanoseconds $=$ 0.0000000076 second

d. $200^2 = 40{,}000$ nanoseconds $= 0.00004$ second

e. $200^8 = 2.56 \times 10^{18}$ nanoseconds $\cong$ $\frac{2.56 \times 10^{18}}{10^9 \cdot 60 \cdot 60 \cdot 24 \cdot (365.25)}$ years $\cong 81.1215$ years

[because there are 10^9 nanoseconds in a second, 60 seconds in a minute, 60 minutes in an hour, 24 hours in a day, and approximately 365.25 days in a year on average].

2. a. When the input size is increased from m to $2m$, the number of operations increases from cm^2 to $c(2m)^2 = 4cm^2$.

b. By part (a), the number of operations increases by a factor of $(4cm^2)/cm^2 = 4$.

c. When the input size is increased by a factor of 10 (from m to $10m$), the number of operations increases by a factor of $(c(10m)^2)/(cm^2) = (100cm^2)/cm^2 = 100$.

4. a. Algorithm A has order n^2 and algorithm B has order $n^{3/2}$.

b. Algorithm A is more efficient than algorithm B when $2n^2 < 80n^{3/2}$. This occurs exactly when

$$n^2 < 40n^{3/2} \Leftrightarrow \frac{n^2}{n^{3/2}} < 40 \Leftrightarrow n^{1/2} < 40 \Leftrightarrow n < 40^2.$$

Thus, algorithm A is more efficient than algorithm B when $n < 40^2 = 1{,}600$.

c. Algorithm B is at least 100 times more efficient than algorithm A for values of n with $100(80n^{3/2}) \leq 2n^2$. This occurs exactly when $8{,}000n^{3/2} \leq 2n^2 \Leftrightarrow 4{,}000 \leq \frac{n^2}{n^{3/2}} \Leftrightarrow 4{,}000 \leq \sqrt{n} \Leftrightarrow 16{,}000{,}000 \leq n$. Thus, algorithm B is at least 100 times more efficient than algorithm A when $n \geq 16{,}000{,}000$.

6. a. There are two multiplications, one addition, and one subtraction for each iteration of the loop, so there are four times as many operations as there are iterations of the loop. The loop is iterated $(n-1) - 3 + 1 = n - 3$ times (since the number of iterations equals the top minus the bottom index plus 1). Thus the total number of operations is $4(n-3) = 4n - 12$.

b. By the theorem on polynomial orders, $4n - 12$ is $\Theta(n)$, so the algorithm segment has order n.

8. a. There is one addition for each iteration of the loop, and there are $\lfloor n/2 \rfloor$ iterations of the loop.

b. Because

$$\lfloor n/2 \rfloor = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (n-1)/2 & \text{if } n \text{ is odd, then } \lfloor n/2 \rfloor \end{cases}$$

is $\Theta(n)$ by theorem on polynomial orders. So the algorithm segment has order n.

9. a. For each iteration of the inner loop, there is one multiplication and one addition. There are $2n$ iterations of the inner loop for each iteration of the outer loop, and there are n iterations of the outer loop. Therefore, the number of iterations of the inner loop is $2n \cdot n = 2n^2$. It follows that the total number of elementary operations that must be performed when the algorithm is executed is $2 \cdot 2n^2 = 4n^2$.

b. Since $4n^2$ is $\Theta(n^2)$ (by the theorem on polynomial orders), the algorithm segment has order n^2.

11. a. There is one addition for each iteration of the inner loop. The number of iterations in the inner loop equals the number of columns in the table below, which shows the values of k and j for which the inner loop is executed.

k	1		2			3				…	$n-1$				
j	1	2	1	2	3	1	2	3	4	…	1	2	3	…	n
		2		3			4					n			

Hence the total number of iterations of the inner loop is

$$2+3+\cdots+n=(1+2+3+\cdots+n)-1$$
$$=\frac{n(n+1)}{2}-1=\frac{n^2+n}{2}-1=\frac{1}{2}n^2+\frac{1}{2}n-1$$

(by Theorem 5.2.1). Because one operation is performed for each iteration of the inner loop, the total number of operations is $\frac{1}{2}n^2+\frac{1}{2}n-1$.

b. By the theorem on polynomial orders, $\frac{1}{2}n^2+\frac{1}{2}n-1$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

14. a. There is one addition for each iteration of the inner loop, and there is one additional addition and one multiplication for each iteration of the outer loop. The number of iterations in the inner loop equals the number of columns in the following table, which shows the values of i and j for which the inner loop is executed.

i	1	2		3			$\cdots$	n				
j	1	1	2	1	2	3	$\cdots$	1	2	3	$\cdots$	n
	1		2			3					n	

Hence the total number of iterations of the inner loop is

$$1+2+3+\cdots+n=(1+2+3+\cdots+n)$$
$$=\frac{n(n+1)}{2}=\frac{n^2+n}{2}=\frac{1}{2}n^2+\frac{1}{2}n$$

(by Theorem 5.2.1). Because one addition is performed for each iteration of the inner loop, the number of operations performed when the inner loop is executed is $\frac{1}{2}n^2+\frac{1}{2}$. Now an additional two operations are performed each time the outer loop is executed, and because the outer loop is executed n times, this gives an additional $2n$ operations. Therefore, the total number of operations is

$$\frac{1}{2}n^2+\frac{1}{2}n+2n=\frac{1}{2}n^2+\frac{5}{2}n.$$

b. By the theorem on polynomial orders, $\frac{1}{2}n^2+\frac{5}{2}n$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

17. a. There are two subtractions and one multiplication for each iteration of the inner loop. If n is odd, the number of iterations of the inner loop equals the number of columns in the following table, which shows the values of i and j for which the inner loop is executed.

Thus the number of iterations of the inner loop is

$$1+1+2+2+\cdots+\frac{n-1}{2}+\frac{n-1}{2}+\frac{n+1}{2}$$
$$=2\cdot\left(1+2+3+\cdots+\frac{n-1}{2}\right)+\frac{n+1}{2}$$
$$=2\cdot\frac{\frac{n-1}{2}\left(\frac{n-1}{2}+1\right)}{2}+\frac{n+1}{2} \quad \text{by Theorem 5.2.1}$$
$$=\frac{n^2-2n+1}{4}+\frac{n-1}{2}+\frac{n-1}{2}$$
$$=\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{4}.$$

By similar reasoning, if n is even, then the number of iterations of the inner loop is

$$1+1+2+2+3+3+\cdots+\frac{n}{2}+\frac{n}{2}$$
$$=2\cdot\left(1+2+3+\cdots+\frac{n}{2}\right)$$
$$=2\cdot\left(\frac{\frac{n}{2}\left(\frac{n}{2}+1\right)}{2}\right) \quad \text{by Theorem 5.2.1}$$
$$=\frac{n^2}{4}+\frac{n}{2}.$$

Because three operations are performed for each iteration of the inner loop, the answer is $3\left(\frac{n^2}{4}+\frac{n}{2}\right)$ when n is even and $3\left(\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{4}\right)$ when n is odd.

b. Since $3\left(\frac{n^2}{4}+\frac{n}{2}\right)$ is $\Theta(n^2)$ and $3\left(\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{4}\right)$ is also $\Theta(n^2)$ (by the theorem on polynomial orders), this algorithm segment has order n^2.

19. *Hint:* See Section 9.6 for a discussion of how to count the number of iterations of the innermost loop.

20.

	$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
Initial order	6	2	1	8	4
Result of step 1	2	6	1	8	4
Result of step 2	1	2	6	8	4
Result of step 3	1	2	6	8	4
Final order	1	2	4	6	8

i	1	2	3		4		5			6			$\cdots$	$n-1$		$\cdots$		n		$\cdots$	
$\left\lfloor\frac{i+1}{2}\right\rfloor$	1	1	2		2		3			3			$\cdots$	$\frac{n-1}{2}$		$\cdots$		$\frac{n+1}{2}$		$\cdots$	
j	1	1	1	2	1	2	1	2	3	1	2	3	$\cdots$	1	2	$\cdots$	$\frac{n-1}{2}$	1	2	$\cdots$	$\frac{n+1}{2}$
	1		1		2		2		3		3			$\frac{n-1}{2}$				$\frac{n+1}{2}$			

22.

n	5									
***a*[1]**	6	2			1					
***a*[2]**	2	6		1	2					
***a*[3]**	1			6					4	
***a*[4]**	8							4	6	
***a*[5]**	4							8		
k	2		3			4		5		
x	2		1			8		4		
j	1	0	2	1	0	3	0	4	3	2	0

24. There are seven comparisons between values of x and values of $a[\,j]$: one $k = 2$, two when $k = 3$, one when $k = 4$, and three when $k = 5$.

27. *Hint:* $E_n = \frac{1}{2}[3 + 4 + \cdots + (n+1)]$, which equals $\frac{1}{2}[(1 + 2 + 3 + \cdots + (n+1)) - (1 + 2)]$.

28. The top row of the table shows the initial values of the array, and the bottom row shows the final values. The results for executing each step in the for-next loop are shown in separate rows.

k	$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
Initial	7	3	8	4	2
1	2	3	8	4	7
2	2	3	8	4	7
3	2	3	4	8	7
4	2	3	4	7	8
5	2	3	4	7	8

30.

n	5													
***a*[1]**	7	3				2								
***a*[2]**	3	7												
***a*[3]**	8										4			
***a*[4]**	4										8			7
***a*[5]**	2					7								8
k	1						2			3		4		
IndexOfMin	1	2			5		2			3	4	4	5	
i	2		3	4	5		3	4	5	4	5	5		
temp						7					8			7

32. There is one comparison for each combination of values of k and i: namely, $4 + 3 + 2 + 1 = 10$.

35. b. $n - 3 + 1 = n - 2$ **d.** *Hint:* The answer is n^2.

36.

n	3									
***a*[0]**	2									
***a*[1]**	1									
***a*[2]**	−1									
***a*[3]**	3									
x	2									
polyval	2		4			0				24
i	1		2			3				
term	1	2	−1	−2	−4	3	6	12	24	
j	1		1	2		1	2	3		

38. Number of multiplications

$$\begin{aligned} &= \text{number of iterations of the inner loop} \\ &= 1 + 2 + 3 + \cdots + n \\ &= \frac{n(n+1)}{2} \quad \text{by Theorem 5.2.1} \end{aligned}$$

Number of additions

$$\begin{aligned} &= \text{number of iterations of the outer loop} \\ &= n \end{aligned}$$

Hence the total number of multiplications and additions is

$$\frac{n(n+1)}{2} + n = \frac{1}{2}n^2 + \frac{3}{2}n.$$

40.

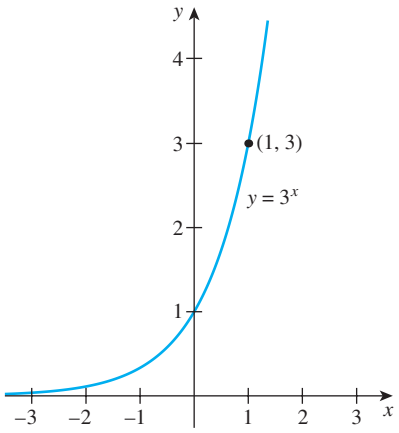
n	3			
***a*[0]**	2			
***a*[1]**	1			
***a*[2]**	−1			
***a*[3]**	3			
x	2			
polyval	3	5	11	24
i	1	2	3	

42. *Hint:* $t_n = 2n$.

SECTION 11.4

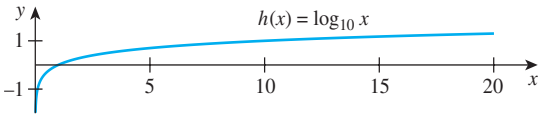
1.

x	$f(x) = 3^x$
0	$3^0 = 1$
1	$3^1 = 3$
2	$3^2 = 9$
−1	$3^{-1} = 1/3$
−2	$3^{-2} = 1/9$
1/2	$3^{1/2} \cong 1.7$
−(1/2)	$3^{-(1/2)} \cong 0.6$



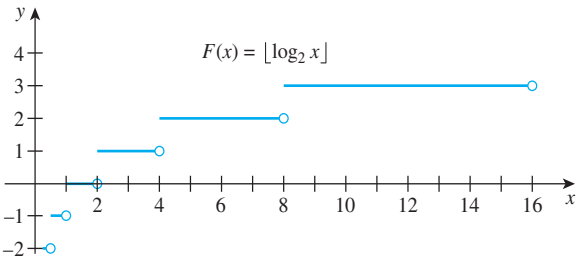
3.

x	$h(x) = \log_{10} x$
1	0
10	1
100	2
1/10	−1
1/100	−2



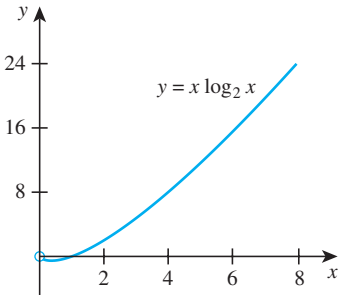
5.

x	$\lfloor \log_2 x \rfloor$
$1 \le x < 2$	0
$2 \le x < 4$	1
$4 \le x < 8$	2
$8 \le x < 16$	3
$1/2 \le x < 1$	−1
$1/4 \le x < 1/2$	−2



7.

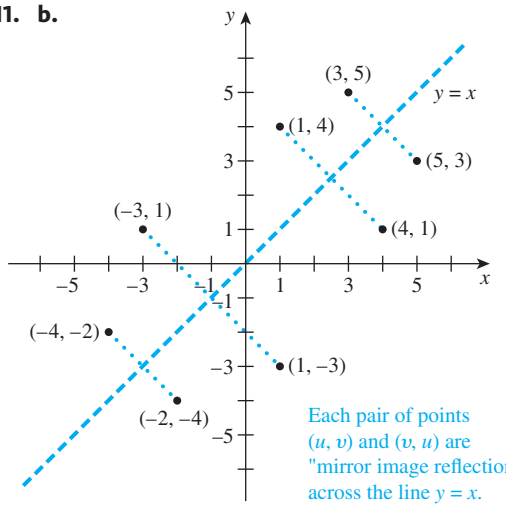
x	$x \log_2 x$
1	$1 \cdot 0 = 0$
2	$2 \cdot 1 = 2$
4	$4 \cdot 2 = 8$
8	$8 \cdot 3 = 24$
1/8	$(1/8) \cdot (-3) = -3/8$
1/4	$(1/4) \cdot (-2) = -1/2$
3/8	$(3/8) \cdot (\log_2(3/8)) \cong -0.53$



9. The distance above the axis is $(2^{64}$ units$) \cdot \left(\frac{1}{4} \frac{\text{inch}}{\text{unit}}\right) = \frac{2^{64}}{4}$ inches $= \frac{2^{64}}{4 \cdot 12 \cdot 5280}$ miles $\cong$ 72,785,448,520,000 miles. The ratio of the height of the point to the average distance of the earth to the sun is approximately 72785448520000/93000000 $\cong$ 782,639. (If you perform the computation using metric units and the approximation 0.635 cm $\cong$ 1/4 inch, the ratio comes out to be approximately 780,912.)

10. b. By definition of logarithm, $\log_b x$ is the exponent to which b must be raised to obtain x. Thus when b is actually raised to this exponent, x is obtained. That is, $b^{\log_b x} = x$.

11. b.



Each pair of points (u, v) and (v, u) are "mirror image reflections" across the line $y = x$.

13. *Hints:* (1) $\lfloor \log_{10} x \rfloor = m$, (2) See Example 11.4.1.

15. No. Counterexample: Let $n = 2$. Then $\lceil \log_2 (n-1) \rceil = \lceil \log_2 1 \rceil = \lceil 0 \rceil = 0$, whereas $\lceil \log_2 n \rceil = \lceil \log_2 2 \rceil = \lceil 1 \rceil = 1$.

16. *Hint:* The statement is true.

18. $\lfloor \log_2 148206 \rfloor + 1 = 18$

21. a. $a_1 = 1$

$a_2 = a_{\lfloor 2/2 \rfloor} + 2 = a_1 + 2 = 1 + 2$

$a_3 = a_{\lfloor 3/2 \rfloor} + 2 = a_1 + 2 = 1 + 2$

$a_4 = a_{\lfloor 4/2 \rfloor} + 2 = a_2 + 2 = (1 + 2) + 2$
$= 1 + 2 \cdot 2$

$a_5 = a_{\lfloor 5/2 \rfloor} + 2 = a_2 + 2 = (1 + 2) + 2$
$= 1 + 2 \cdot 2$

$a_6 = a_{\lfloor 6/2 \rfloor} + 2 = a_3 + 2 = (1 + 2) + 2$
$= 1 + 2 \cdot 2$

$a_7 = a_{\lfloor 7/2 \rfloor} + 2 = a_3 + 2 = (1 + 2) + 2$
$= 1 + 2 \cdot 2$

$a_8 = a_{\lfloor 8/2 \rfloor} + 2 = a_4 + 2$
$= (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$

$a_9 = a_{\lfloor 9/2 \rfloor} + 2 = a_4 + 2$
$= (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$

$\vdots$

$a_{15} = a_{\lfloor 15/2 \rfloor} + 2 = a_7 + 2$
$= (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$

$a_{16} = a_{\lfloor 16/2 \rfloor} + 2 = a_8 + 2$
$= (1 + 3 \cdot 2) + 2 = 1 + 4 \cdot 2$

Guess:
$a_n = 1 + 2 \lfloor \log_2 n \rfloor$

b. Proof: Suppose the sequence $a_1, a_2, a_3, \ldots$ is defined recursively as follows: $a_1 = 1$ and $a_k = a_{\lfloor k/2 \rfloor} + 2$ for each integer $k \geq 2$. Let the property $P(n)$ be the equation $a_n = 1 + 2 \lfloor \log_2 n \rfloor$. We will show by strong mathematical induction that $P(n)$, is true for each integer $n \geq 1$.

Show that P(1) is true: $P(1)$ is the equation $1 + 2\lfloor \log_2 1 \rfloor = 1 + 2 \cdot 0 = 1$, which is the value of a_1.

Show that for any integer k ≥ 1, if P(i) is true for every integer i from 1 through k, then P(k + 1) is true: Let k be any integer with $k \geq 1$, and suppose $a_i = 1 + 2\lfloor \log_2 i \rfloor$ for each integer i from 1 through k. *[This is the inductive hypothesis.]* We must show that $a_{k+1} = 1 + 2\lfloor \log_2 (k+1) \rfloor$.

Case 1 (k is odd): In this case $k + 1$ is even, and

$a_{k+1} = a_{\lfloor (k+1)/2 \rfloor} + 2$
by the recursive definition of $a_1, a_2, a_3, \ldots$
$= a_{(k+1)/2} + 2$
because $k + 1$ is even (Theorem 4.6.2)
$= 1 + 2\lfloor \log_2 ((k+1)/2) \rfloor + 2$
by inductive hypothesis
$= 3 + 2\lfloor \log_2 (k+1) - \log_2 2 \rfloor$
by Theorem 7.2.1(b)
$= 3 + 2\lfloor \log_2 (k+1) - 1) \rfloor$
because $\log_2 2 = 1$
$= 3 + 2(\lfloor \log_2 (k+1) \rfloor - 1)$
because for every real number x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$
by exercise 15, Section 4.6
$= 1 + 2\lfloor \log_2 (k+1) \rfloor$
by algebra.

Case 2 (k is even): In this case $k + 1$ is odd, and

$a_{k+1} = a_{\lfloor (k+1)/2 \rfloor} + 2$
by the recursive definition of $a_1, a_2, a_3, \ldots$
$= a_{k/2} + 2$
by Theorem 4.6.2 because $k + 1$ is odd.
$= 1 + 2\lfloor \log_2 (k/2) \rfloor + 2$
by inductive hypothesis
$= 3 + 2\lfloor \log_2 k - \log_2 2 \rfloor$
by Theorem 7.2.1(b)
$= 3 + 2\lfloor \log_2 k - 1 \rfloor$
because $\log_2 2 = 1$
$= 3 + 2(\lfloor \log_2 k \rfloor - 1)$
because for every real number x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$
by exercise 15, Section 4.6
$= 1 + 2\lfloor \log_2 k \rfloor$
by algebra.
$= 1 + 2\lfloor \log_2 (k+1) \rfloor$
by property 11.4.3.

Thus in either case, $a_{k+1} = 1 + 2\lfloor \log_2 (k+1) \rfloor$ *[as was to be shown].*

23. *Hint:* When $k \geq 2$, then $k^2 \geq 2k$, and so $k \leq \frac{k^2}{2}$. Hence $\frac{k^2}{2} + k \leq \frac{k^2}{2} + \frac{k^2}{2} = k^2$. Also, when $k \geq 2$ then $k^2 > 1$, and so $\frac{1}{2} < \frac{k^2}{2}$. Consequently, $\frac{k^2}{2} + \frac{1}{2} < \frac{k^2}{2} + \frac{k^2}{2} = k^2$.

24. *Hint:* Here is the argument for the inductive step in the case where k is odd and $k + 1$ is even.

$c_{k+1} = 2c_{\lfloor (k+1)/2 \rfloor} + (k+1)$
by the recursive definition of $c_1, c_2, c_3, \ldots$
$= 2c_{(k+1)/2} + (k+1)$
by Theorem 4.6.2 because $k + 1$ is even
$\leq 2\left[\frac{k+1}{2} \log_2 \left(\frac{k+1}{2}\right)\right] + (k+1)$
by inductive hypothesis
$= (k+1)[\log_2 (k+1) - \log_2 2] + (k+1)$
by algebra and Theorem 7.2.1(b)
$= (k+1)[\log_2 (k+1) - 1] + (k+1)$
because $\log_2 2 = 1$
$= (k+1)(\log_2 (k+1))$
by algebra.

25. *Solution 1:* One way to solve this problem is to compare values for $\log_2 x$ and $x^{1/10}$ for conveniently chosen, large values of x. For instance, if powers of 10 are used, the following results are obtained: $\log_2 (10^{10}) = 10 \log_2 10 \cong 33.2$ and $(10^{10})^{1/10} = 10^{10 \cdot (1/10)} = 10^1 = 10$. Thus the value $x = 10^{10}$ does not work.

However, since $\log_2(10^{20}) = 20\log_2 10 = 66.4$ and $(10^{20})^{1/10} = 10^{20\cdot(1/10)} = 10^2 = 100$, and since $66.4 < 100$, the value $x = 10^{20}$ works.

Solution 2: Another approach is to use a graphing calculator or computer to sketch graphs of $y = \log_2 x$ and $y = x^{1/10}$, taking seriously the hint to "think big" in choosing the interval size for the x's. A few tries and use of the zoom and trace features make it appear that the graph of $y = x^{1/10}$ crosses above the graph of $y = \log_2 x$ at about 4.9155×10^{17}. Thus, for values of x larger than this, $x^{1/10} > \log_2 x$.

27. By Theorem 11.2.7, n is $\Theta(n)$ and $\log_2 n$ is $\Theta(\log_2 n)$, and, by Theorem 11.2.8(c), $2n$ is $\Theta(n)$. In addition, by property 11.4.9, there is a positive real number s such that for each integer $n \geq s$, $\log_2 n \leq n$. Finally, if n is any integer with $n \geq 1$, then $n \geq 0$. Thus it follows from Theorem 11.2.9(c) that $2n + \log_2 n$ is $\Theta(n)$.

29. By Theorem 11.2.7, n^2 is $\Theta(n^2)$ and 2^n is $\Theta(2^n)$. In addition, by property 11.4.10, there is a positive real number s such that for each integer $n \geq s$, $n^2 \leq 2^n$. Finally, if n is any integer, then $2^n \geq 0$. Thus it follows from Theorem 11.2.9(c) that $n^2 + 2^n$ is $\Theta(2^n)$.

30. *Hint:* $2^{n+1} = 2\cdot 2^n$

31. *Hint:* Use a proof by contradiction. Start by supposing that 4^n is $O(2^n)$. That is, that there are positive real numbers B and b such that $O \leq 4^n \leq B\cdot 2^n$ for every real number $n > b$, and use the fact that $\frac{4^n}{2^n} = \left(\frac{4}{2}\right)^n = 2^n$ to obtain a contradiction.

32. By Theorem 5.2.2, for each integer $n \geq 0$,

$$1 + 2 + 2^2 + \cdots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

Also,

$$2^n \leq 2^{n+1} - 1 \leq 2^{n+1} = 2\cdot 2^n.$$

Thus, by transitivity of order,

$$2^n \leq 1 + 2 + 2^2 + \cdots + 2^n \leq 2\cdot 2^n.$$

Moreover,

$$2^n \geq 0 \text{ for each integer } n.$$

Let $A = 1$, $B = 2$, and $k = 1$. Then, for each integer $n > k$,

$$A\cdot 2^n \leq 1 + 2 + 2^2 + \cdots + 2^n \leq B\cdot 2^n.$$

Thus, by definition of Θ-notation, $1 + 2 + 2^2 + \cdots + 2^n$ is $\Theta(2^n)$.

33. *Hint:* This is similar to the solution for exercise 32. Use the fact that $4 + 4^2 + 4^3 + \cdots + 4^n = 4(1 + 4 + 4^2 + 4^3 + \cdots + 4^{n-1})$.

36. Factor out n to obtain

$$\begin{aligned}
&n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n} \\
&\quad = n\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n}\right) \\
&\quad = n\left(\frac{\left(\frac{1}{2}\right)^{n+1} - 1}{\frac{1}{2} - 1}\right) && \text{by Theorem 5.2.2} \\
&\quad = n\left(\frac{1 - 2^{n+1}}{2^n(1-2)}\right) && \text{by multiplying numerator and denominator by } 2^{n+1} \\
&\quad = n\left(\frac{2^{n+1} - 1}{2^n}\right) \\
&\quad = n\left(2 - \frac{1}{2^n}\right) && \text{by algebra.}
\end{aligned}$$

Now $1 \leq 2 - \frac{1}{2^n} \leq 2$ when $n > 1$. Thus

$$1\cdot n \leq n\left(2 - \frac{1}{2^n}\right) \leq 2\cdot n,$$

and so, by substitution,

$$1\cdot n \leq n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n} \leq 2\cdot n.$$

Let $A = 1$, $B = 2$, and $k = 1$. Then, for each integer $n > k$,

$$A\cdot n \leq n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n} \leq B\cdot n.$$

Hence, by definition of Θ-notation,

$$n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n} \text{ is } \Theta(n).$$

40. If n is any integer with $n \geq 3$, then

$$n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} = n\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right).$$

By Example 11.4.7 and by Theorem 11.2.7(a),

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \text{ is } \Theta(\log_2 n) \quad \text{and} \quad n \text{ is } \Theta(n).$$

Thus, by Theorem 11.2.9(c),

$$n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} \text{ is } \Theta(n \log_2 n).$$

41. Proof: If n is any positive integer, then $\log_2 n$ is defined and by definition of floor,

$$\lfloor \log_2 n \rfloor \leq \log_2 n < \lfloor \log_2 n \rfloor + 1.$$

If, in addition, n is greater than 2, then since the logarithmic function with base 2 is increasing

$$\log_2 n > \log_2 2 = 1.$$

Thus, by definition of floor,

$$1 \leq \lfloor \log_2 n \rfloor.$$

Adding $\lfloor \log_2 n \rfloor$ to both sides of this inequality gives

$$\lfloor \log_2 n \rfloor + 1 \le 2 \lfloor \log_2 n \rfloor.$$

Hence, by the transitive property of order (T18 in Appendix A),

$$\log_2 n \le 2 \lfloor \log_2 n \rfloor,$$

and dividing both sides by 2 gives

$$\frac{1}{2} \log_2 n \le \lfloor \log_2 n \rfloor.$$

Let $A = 1/2$, $B = 1$, and $k = 2$. Then

$A \log_2 n \le \lfloor \log_2 n \rfloor \le B \log_2 n$ for every integer $n \ge k$.

Therefore, by definition of Θ-notation, $\lfloor \log_2 n \rfloor$ is $\Theta(\log_2 n)$.

43. Proof (by mathematical induction): Let the property $P(n)$ be the inequality $n \le 10^n$.

Show that P(1) is true:

When $n = 1$, the inequality is $1 \le 10$, which is true.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

Let k be any integer with $k \ge 1$, and suppose $k \le 10^k$. *[This is the inductive hypothesis.]* We must show that $k + 1 \le 10^{k+1}$. By inductive hypothesis, $k \le 10^k$. Adding to both sides gives $k + 1 \le 10^k + 1$. But when $k \ge 1$, $10^k + 1 \le 10^k + 9 \cdot 10^k = 10 \cdot 10^k = 10^{k+1}$. Thus, by transitivity of order, $k + 1 \le 10^{k+1}$ *[as was to be shown].*

44. *Hint:* To prove the inductive step, use the fact that if $k > 1$, then $k + 1 \le 2k$. Apply the logarithmic function with base 2 to both sides of this inequality, and use properties of logarithms.

45. *Hint:* $\underbrace{2 \cdot 2 \cdot 2 \ldots 2}_{n \text{ factors}} \le 2 \cdot (2 \cdot 3 \cdot 4 \ldots n) = 2 \cdot n!$

46. a. Example 11.4.6 showed that if n is any integer with $n \ge 1$, then $n! \le n^n$. So, because the logarithmic function with base 2 is increasing,

$$\log_2(n!) \le \log_2(n^n) \; (= n \log_2(n^n)).$$

Also, when $n \ge 1$, then $\log_2(n!) \ge \log_2 1 \ge 0$. Thus let $B = 1$ and $b = 1$. Then

$0 \le \log_2(n!) \le Bn \log_2(n^n)$ for every integer $n \ge b$.

So, by definition of O-notation, $\log_2(n!)$ is $O(n \log_2 n)$.

b. *Hint:*

$$(n!)^2 = n! \cdot n! = (1 \cdot 2 \cdot 3 \cdots 3)(n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1)$$

$$= \left(\prod_{r=1}^{n} r \right) \left(\prod_{r=1}^{n} (n - r + 1) \right) = \prod_{r=1}^{n} r(n - r + 1).$$

Show that for each integer $r = 1, 2, \ldots, n$, $nr - n^2 + r \ge n$.

47. Let n be a positive integer, and suppose that $x > (2^n)^{2n}$. By properties of logarithms,

$$\log_2 x = (2n)\left(\frac{1}{2n}\right)(\log_2 x)$$

$$= (2n) \log_2\left(x^{\frac{1}{2n}}\right) < 2n x^{\frac{1}{2n}} \qquad (*)$$

(where the last inequality holds by substituting $x^{\frac{1}{2n}}$ in place of u in $\log_2 u < u$). Now raising both sides of $x > (2n)^{2n}$ to the 1/2 power gives $x^{1/2} > ((2n)^{2n})^{1/2} = (2n)^n$. When both sides are multiplied by $x^{1/2}$, the result is $x = x^{1/2}x^{1/2} > x^{1/2}(2n)^n = x^{1/2}(2n)^n$, or, more compactly,

$$x^{1/2}(2n)^n < x.$$

Then, since the power function defined by $x \to x^{1/n}$ is increasing for every $x > 0$ (see exercise 21 of Section 11.1), we can take the nth root of both sides of the inequality and use the laws of exponents to obtain

$$(x^{1/2}(2n)^n)^{1/n} < x^{1/n},$$

or, equivalently,

$$2n x^{\frac{1}{2n}} < x^{1/n}. \qquad (**)$$

Finally use transitivity of order (Appendix A, T18) to combine (*) and (**) and conclude that $\log_2 x < x^{1/n}$ *[as was to be shown].*

49. a. Proof (by mathematical induction): Let b be any real number with $b > 1$, and let the property $P(n)$ be the equation

$$\lim_{x \to \infty} \left(\frac{x^n}{b^x} \right) = 0.$$

Show that P(1) is true:

By L'Hôpital's rule, $\lim_{x \to \infty} \left(\frac{x^1}{b^x} \right) = \lim_{x \to \infty} \left(\frac{1}{b^x (\ln b)} \right) = 0$.

Thus $P(1)$ is true.

Show that for every integer k ≥ 1, if P(k) is true, then P(k + 1) is true:

Let k be any integer with $k \ge 1$, and suppose $\lim_{x \to \infty} \left(\frac{x^k}{b^x} \right) = 0$. *[This is the inductive hypothesis.]*

We must show that $\lim_{x \to \infty} \left(\frac{x^{k+1}}{b^x} \right) = 0$. Now by L'Hôpital's rule, $\lim_{x \to \infty} \left(\frac{x^{k+1}}{b^x} \right) = \lim_{x \to \infty} \frac{(k+1)x^k}{(\ln b) b^x} = \frac{(k+1)}{(\ln b)} \left[\lim_{x \to \infty} \frac{x^k}{b^x} \right] = \frac{(k+1)}{(\ln b)} \cdot 0$ *[by inductive hypothesis]* $= 0$.

[This is what was to be shown.]

b. By the result of part (a) and the definition of limit, given any real number $\varepsilon > 0$, there exists an integer N such that $\left| \frac{x^n}{b^n} - 0 \right| < \varepsilon$ for every $x > N$. In this case take $\varepsilon = 1$. It follows that for every $x > N$, $\frac{x^n}{b^x} < 1$ since x and b are positive. Multiply both sides by b^x to obtain $x^n < b^x$. Let $B = 1$. Then $0 < x^n < B \cdot b^x$ for every $x > N$. Hence, by definition of O-notation, x^n is $O(b^x)$.

SECTION 11.5

1. $\log_2 1{,}000 = \log_2(10^3) = 3 \log_2 10 \cong 3(3.32) \cong 9.96$

$\log_2(1{,}000{,}000) = \log_2(10^6) = 6 \log_2 10 \cong 6(3.32) \cong 19.92$

$\log_2(1{,}000{,}000{,}000{,}000) = \log_2(10^{12}) = 12 \log_2 10 \cong 12(3.32) = 39.84$

2. a. If $m = 2^k$, where k is a positive integer, then the algorithm requires $c\lfloor \log_2(2^k) \rfloor = c\lfloor k \rfloor = ck$ operations. If the input size is increased to $m^2 = (2^k)^2 = 2^{2k}$, then the number of operations required is $c\lfloor \log_2(2^{2k}) \rfloor = c\lfloor 2k \rfloor = 2(ck)$. Hence the number of operations doubles.

b. As in part (a), for an input of size $m = 2^k$, where k is a positive integer, the algorithm requires ck operations. If the input size is increased to $m^{10} = (2^k)^{10} = 2^{10k}$, then the number of operations required is $c\lfloor \log_2(2^{10k}) \rfloor = c\lfloor 10k \rfloor = 10(ck)$. Thus the number of operations increases by a factor of 10.

c. When the input size is increased from 2^7 to 2^{28}, the factor by which the number of operations increases is $\dfrac{c\lfloor \log_2(2^{28}) \rfloor}{c\lfloor \log_2(2^7) \rfloor} = \dfrac{28c}{7c} = 4$.

3. A little numerical exploration can help find an initial window to use to draw the graphs of $y = x$ and $y = \lfloor 50 \log_2 x \rfloor$. Note that when $x = 2^8 = 256$, $\lfloor 50 \log_2 x \rfloor = \lfloor 50 \log_2(2^8) \rfloor = \lfloor 50 \cdot 8 \rfloor = \lfloor 400 \rfloor = 400 > 256 = x$. But when $x = 2^9 = 512$, $\lfloor 50 \log_2 x \rfloor = \lfloor 50 \log_2(2^9) \rfloor = \lfloor 50 \cdot 9 \rfloor = \lfloor 450 \rfloor = 450 < 512 = x$. So a good choice of initial window would be the interval from 256 to 512. Drawing the graphs, zooming if necessary, and using the trace feature reveal that when $n < 438$, $n < \lfloor 50 \log_2 n \rfloor$.

5. a.

index	0			1
bot	1			
top	10	4	1	
mid		5	2	1
x	Chia			

b.

index	0				
bot	1	6		7	
top	10		7		6
mid		5	8	6	7
x	Max				

7. a. The array has $top - bot + 1$ elements.

b. Proof: Suppose top and bot are particular but arbitrarily chosen positive integers such that $top - bot + 1$ is an odd number. Then, by definition of odd, there is an integer k such that

$$top - bot + 1 = 2k + 1.$$

Adding $2 \cdot bot - 1$ to both sides gives

$$\begin{aligned} bot + top &= 2 \cdot bot - 1 + 2k + 1 \\ &= 2(bot + k). \end{aligned}$$

Now $bot + k$ is an integer. Hence, by definition of even, $bot + top$ is even.

8.

n	27	13	6	3	1	0

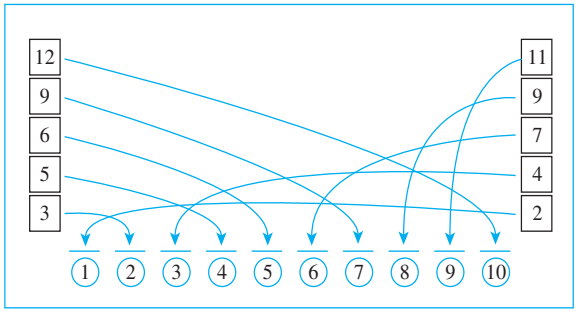
9. For each positive integer n, $n \; div \; 2 = \lfloor n/2 \rfloor$. Thus when the algorithm segment is run for a particular n and the **while** loop has iterated one time, the input to the next iteration is $\lfloor n/2 \rfloor$. It follows that the number of iterations of the loop for n is one more than the number of iterations for $\lfloor n/2 \rfloor$. That is, $a_n = 1 + a_{\lfloor n/2 \rfloor}$. Also, $a_1 = 1$.

10. The recurrence relation and initial condition of $a_1, a_2, a_3, \ldots$ derived in exercise 9 are the same as those for the sequence $w_1, w_2, w_3, \ldots$ discussed in the worst-case analysis of the binary search algorithm. Thus the general formulas for the two sequences are the same. That is, $a_n = 1 + \lfloor \log_2 n \rfloor$, for each integer $n \geq 1$.

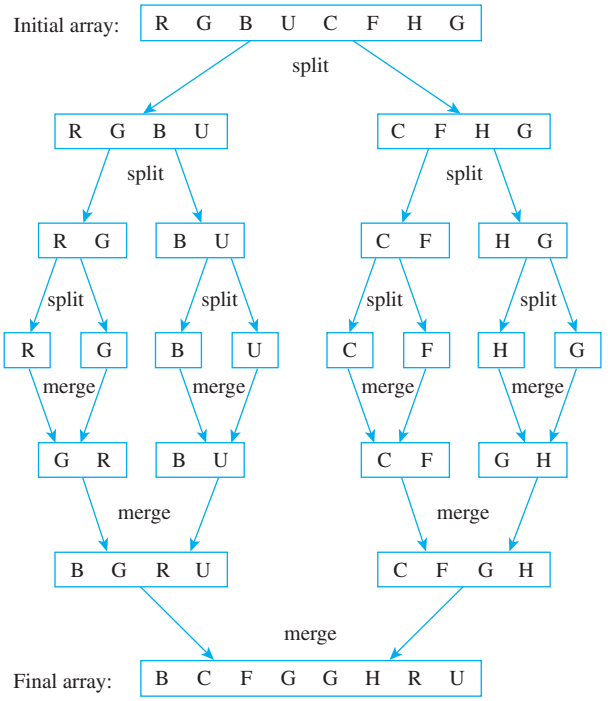
11. In the analysis of the binary search algorithm, it was shown that $1 + \lfloor \log_2 n \rfloor$ is $\Theta(\log_2 n)$. Thus the given algorithm segment has order $\log_2 n$.

14. *Hint:* The formula is $b_n = 1 + \lfloor \log_3 n \rfloor$.

20.



22.



24. a. Refer to Figure 11.5.3 and observe that when k is even, the subarray $a[mid]$, $a[mid+1]$, . . . , $a[top]$ has length $k-\left(\frac{k}{2}+1\right)+1=\frac{k}{2}=\left\lceil\frac{k}{2}\right\rceil$.

25. *Hint:* The following are the steps for part (a) in the case where k is odd and $k+1$ is even:

$$\begin{aligned}
m_{k+1} &= m_{\lfloor (k+1)/2\rfloor}+m_{\lceil (k+1)/2\rceil}+(k+1)-1\\
&= m_{(k+1)/2}+m_{(k+1)/2}+(k+1)-1\\
&\qquad \text{by Theorem 4.6.2 and exercise 19 in Section 4.6 because } k+1 \text{ is even}\\
&= 2m_{(k+1)/2}+k\\
&\geq 2\cdot\left[\frac{1}{2}\cdot\left(\frac{(k+1)}{2}\right)\log_2\left(\frac{k+1}{2}\right)\right]+k\\
&\qquad \text{by inductive hypothesis}\\
&\geq \left(\frac{k+1}{2}\right)[\log_2(k+1)-\log_2 2]+k\\
&\geq \frac{1}{2}(k+1)[\log_2(k+1)-1]+k\\
&\geq \frac{1}{2}(k+1)\log_2(k+1)-1\left(\frac{k+1}{2}\right)+\frac{2k}{2}\\
&\geq \frac{1}{2}(k+1)\log_2(k+1)+\frac{k-1}{2}\\
&\geq \frac{1}{2}(k+1)\log_2(k+1) \qquad \text{by algebra.}
\end{aligned}$$

SECTION 12.1

1. a. $L_1=\{\lambda, x, y, xx, yy, xxx, xyx, yxy, yyy, xxxx, xyyx, yxxy, yyyy\}$

b. $L_2=\{x, xx, xy, xxx, xxy, xyx, xyy\}$

3. a. $(a+b)\cdot(c+d)$

b. *Partial answer:* $11^*=1\cdot 1=1$, $12^*=1\cdot 2=2$, $21/=2/1=2$

4. L_1L_2 is the set of all strings of a's and b's that start with an a and contain an odd number of a's.
$L_1\cup L_2$ is the set of all strings of a's and b's that contain an even number of a's or that start with an a and contain only that one a. (Note that because 0 is an even number, both λ and b are in $L_1\cup L_2$.)
$(L_1\cup L_2)^*$ is the set of all strings of a's and b's. The reason is that a and b are both in $L_1\cup L_2$, and thus every string in a and b is in $(L_1\cup L_2)^*$.

7. $(a\mid((b^*)b))((a^*)\mid(ab))$

10. $(ab^*\mid cb^*)(ac\mid bc)$

13. $$\begin{aligned}L(\lambda\mid ab) &= L(\lambda)\cup L(ab)=\{\lambda\}\cup L(a)L(b)\\ &=\{\lambda\}\cup\{xy\mid x\in L(a)\text{ and }y\in L(b)\}\\ &=\{\lambda\}\cup\{xy\mid x\in\{a\}\text{ and }y\in\{b\}\}\\ &=\{\lambda\}\cup\{ab\}=\{\lambda, ab\}\end{aligned}$$

16. Here is a sample of five strings out of infinitely many: 0101, 1, 01, 10000, and 011100.

19. The language consists of all strings of a's and b's that contain exactly three a's and end in an a.

22. *aaaba* is in the language but *baabb* is not because if a string in the language contains a b to the right of the left-most a, then it must contain another a to the right of all the b's.

25. One solution is $0^*10^*(0^*10^*10^*)^*$.

28. $$\begin{aligned}&L((r\mid s)t)=L(r\mid s)L(t)=(L(r)\cup L(s))L(t)\\ &=\{xy\mid(x\in L(r)\cup L(s))\text{ and }y\in L(t)\}\\ &=\{xy\mid(x\in L(r)\text{ or }x\in L(s))\text{ and }y\in L(t)\}\\ &=\{xy\mid(x\in L(r)\text{ and }y\in L(t))\text{ or }(x\in L(s)\text{ and }y\in L(t))\}\\ &=\{xy\mid xy\in L(rt)\text{ or }xy\in L(st)\}\\ &=L(rt)\cup L(st)=L(rt\mid st)\end{aligned}$$

31. $pre[a-z]^+$

34. $[a-z]^*(a\mid e\mid i\mid o\mid u)[a-z]^*$

37. $[0-9]\{3\}$-$[0-9]\{2\}$-3$[0-9]\{2\}6$

39. $([+\ -]\mid\lambda)[0-9]^*(\backslash.\mid\lambda)[0-9]^*$

40. *Hint:* Leap years from 1980 to 2079 are 1980, 1984, 1988, 1992, 1996, 2000, 2004, and so forth. Note that the fourth digit is 0, 4, or 8 for the years whose third digit is even and that the fourth digit is 2 or 6 for the years whose third digit is odd.

SECTION 12.2

1. a. \$1 or more deposited

2. a. s_0, s_1, s_2 **b.** 0, 1 **c.** s_0 **d.** s_2
e. Annotated next-state table:

State		Input 0	Input 1
	→ s_0	s_1	s_0
	s_1	s_1	s_2
	◎ s_2	s_2	s_2

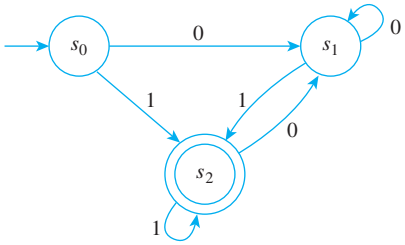
5. a. A, B, C, D, E, F **b.** x, y **c.** A **d.** D, E
e. Annotated next-state table:

State		Input x	Input y
	→ A	C	B
	B	F	D
	C	E	F
	◎ D	F	D
	◎ E	E	F
	F	F	F

7. **a.** s_0, s_1, s_2, s_3 **b.** 0, 1 **c.** s_0 **d.** s_0, s_2
e. Annotated next-state table:

		Input	
		0	1
→	◎ s_0	s_0	s_1
State	s_1	s_1	s_2
	◎ s_2	s_2	s_3
	s_3	s_3	s_0

8. **a.** s_0, s_1, s_2 **b.** 0, 1 **c.** s_0 **d.** s_2
e.



10. **a.** $N(s_1, 1) = s_2$, $N(s_0, 1) = s_3$
c. $N^*(s_0, 10011) = s_2$, $N^*(s_1, 01001) = s_2$

11. **a.** $N(s_3, 0) = s_4$, $N(s_2, 1) = s_4$
c. $N^*(s_0, 010011) = s_3$, $N^*(s_3, 01101) = s_4$

Note that multiple correct answers exist for part (d) of exercises 12 and 13, part (b) of exercises 14–19, and for exercises 20–48.

12. **a.** (i) s_2 (ii) s_2 (iii) s_1
b. those in (i) and (ii) but not (iii)
c. The language accepted by this automaton is the set of all strings of 0's and 1's that contain at least one 0 followed (not necessarily immediately) by at least one 1.
d. $1^*00^*1(0 \mid 1)^*$

14. **a.** The language accepted by this automaton is the set of all strings of 0's and 1's that end in 00.
b. $(0 \mid 1)^*00$

15. **a.** The language accepted by this automaton is the set of all strings of x's and y's of length at least two that consist either entirely of x's or entirely of y's.
b. $xxx^* \mid yyy^*$

17. **a.** The language accepted by this automaton is the set of all strings of 0's and 1's with the following property: If n is the number of 1's in the string, then $n \bmod 4 = 0$ or $n \bmod 4 = 2$. This is equivalent to saying that n is even.
b. $0^* \mid (0^*10^*10^*)^*$

18. **a.** The language accepted by this automaton is the set of all strings of 0's and 1's that end in 1.
b. $(0 \mid 1)^*1$

20. **a.** Call the automaton being constructed A. Acceptance of a string by A depends on the values of three consecutive inputs. Thus A requires at least four states:

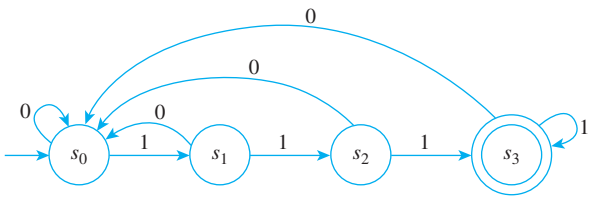
s_0: initial state

s_1: state indicating that the last input character was a 1

s_2: state indicating that the last two input characters were 1's

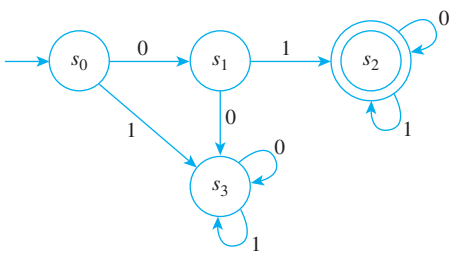
s_3: state indicating that the last three input characters were 1's, the acceptance state

If a 0 is input to A when it is in state s_0, no progress is made toward achieving a string of three consecutive 1's. Hence A should remain in state s_0. If a 1 is input to A when it is in state s_0, it goes to state s_1, which indicates that the last input character of the string is a 1. From state s_1, A goes to state s_2 if a 1 is input. This indicates that the last two characters of the string are 1's. But if a 0 is input, A should return to s_0 because the wait for a string of three consecutive 1's must start over again. When A is in state s_2 and a 1 is input, then a string of three consecutive 1's is achieved, so A should go to state s_3. If a 0 is input when A is in state s_2, then progress toward accumulating a sequence of three consecutive 1's is lost, so A should return to s_0. When A is in a state s_3 and a 1 is input, then the final three symbols of the input string are 1's, and so A should stay in state s_3. If a 0 is input when A is in state s_3, then A should return to state s_0 to await the input of more 1's. Thus the transition diagram is as follows:



b. $(0 \mid 1)^*111$

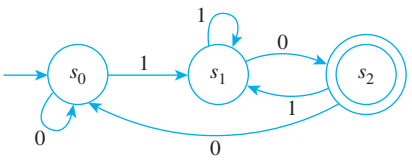
21. **a.**



b. $01(0 \mid 1)^*$

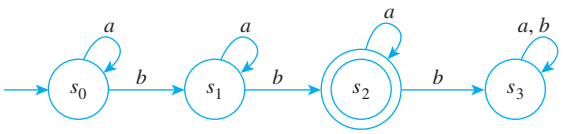
22. *Hint:* Use five states: s_0 (the initial state), s_1 (the state indicating that the previous input symbol was an a), s_2 (the state indicating that the previous input symbol was a b), s_3 (the state indicating that the previous two input symbols were a's), and s_4 (the state indicating that the previous two input symbols were b's).

25. a.



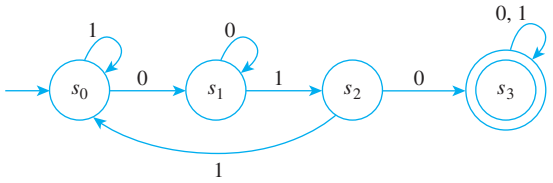
b. $(0 \mid 1)^*10$

26. a.



b. $a^*ba^*ba^*$

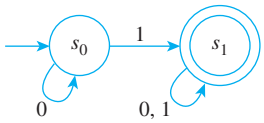
28.



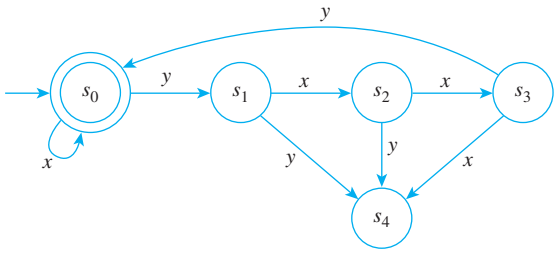
a.

b. $(0 \mid 1)^*010(0 \mid 1)^*$

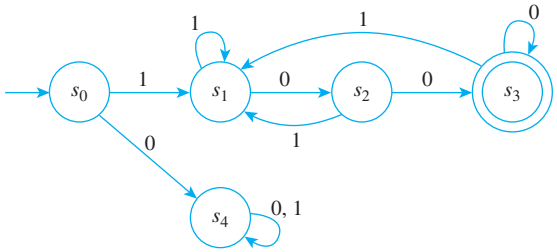
29.



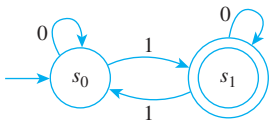
31.



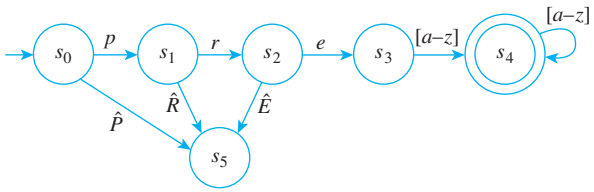
33.



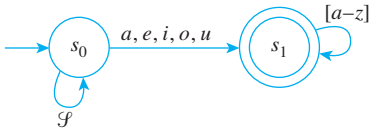
36.



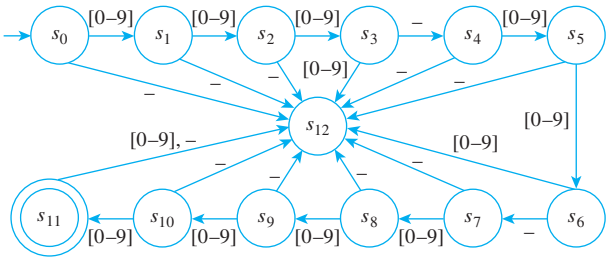
39. Let $\hat{P}$ denote a list of all letters of a lowercase alphabet except p, $\hat{R}$ denote a list of all the letters of a lowercase alphabet except r, and $\hat{E}$ denote a list of all the letters of a lowercase alphabet except e.



42. Let $\mathcal{S}$ denote a list of all the consonants in a lowercase alphabet.



45.



51. *Hint:* This proof is virtually identical to that of Example 12.2.8. Just take p and q in that proof so that $p > q$. From the fact that A accepts $a^p b^p$, you can deduce that A accepts $a^q b^p$. Since $p > q$, this string is not in L.

53. *Hint:* Suppose the automaton A has N states. Choose an integer m such that $(m+1)^2 - m^2 > N$. Consider strings of a's of lengths between m^2 and $(m+1)^2$.
Since there are more strings than states, at least two strings must send A to the same state s_i:

$$\overbrace{\underbrace{aa\ldots aa}_{m^2}a\ldots aa\ldots aa\ldots a}^{(m+1)^2}$$

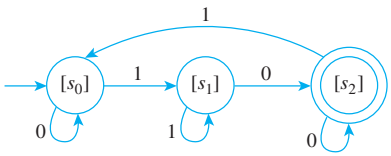
after both of these inputs, A is in state s_i

It follows (by removing the a's shown in color) that the automaton must accept a string of the form a^k, where $m^2 < k < (m+1)^2$.

SECTION 12.3

1. a. 0-equivalence classes: $\{s_0, s_1, s_3, s_4\}$, $\{s_2, s_5\}$
1-equivalence classes: $\{s_0, s_3\}$, $\{s_1, s_4\}$, $\{s_2, s_5\}$
2-equivalence classes: $\{s_0, s_3\}$, $\{s_1, s_4\}$, $\{s_2, s_5\}$

b.



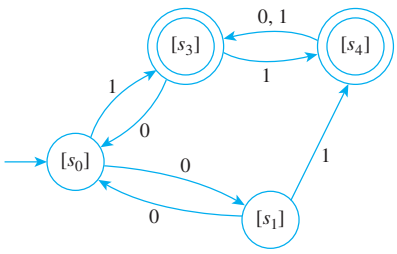
4. a. 0-equivalence classes: $\{s_0, s_1, s_2\}$, $\{s_3, s_4, s_5\}$

1-equivalence classes: $\{s_0, s_1, s_2\}$, $\{s_3, s_5\}$, $\{s_4\}$

2-equivalence classes: $\{s_0, s_2\}$, $\{s_1\}$, $\{s_3, s_5\}$, $\{s_4\}$

3-equivalence classes: $\{s_0, s_2\}$, $\{s_1\}$, $\{s_3, s_5\}$, $\{s_4\}$

b.



6. a. *Hint:* The 3-equivalence classes are $\{s_0\}$, $\{s_1\}$, $\{s_2\}$, $\{s_3\}$, $\{s_4\}$, $\{s_5\}$, and $\{s_6\}$.

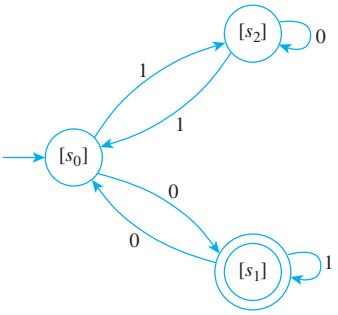
7. Yes. For A:

0-equivalence classes: $\{s_0, s_2\}$, $\{s_1, s_3\}$

1-equivalence classes: $\{s_0\}$, $\{s_2\}$, $\{s_1, s_3\}$

2-equivalence classes: $\{s_0\}$, $\{s_2\}$, $\{s_1, s_3\}$

Transition diagram for $\overline{A}$:



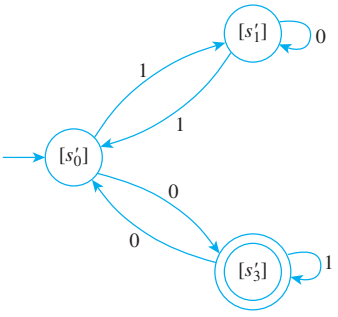
For A':

0-equivalence classes: $\{s'_0, s'_1, s'_2\}$, $\{s'_3\}$

1-equivalence classes: $\{s'_0, s'_2\}$, $\{s'_1\}$, $\{s'_3\}$

2-equivalence classes: $\{s'_0, s'_2\}$, $\{s'_1\}$, $\{s'_3\}$

Transition diagram for $\overline{A'}$:



Except for the labeling of the states, the transition diagrams for $\overline{A}$ and $\overline{A'}$ are identical. Hence $\overline{A}$ and $\overline{A'}$ accept the same language, and so, by Theorem 12.3.3, A and A' also accept the same language. Thus A and A' are equivalent automata.

9. For A:

0-equivalence classes: $\{s_1, s_2, s_4, s_5\}$, $\{s_0, s_3\}$

1-equivalence classes: $\{s_1, s_2\}$, $\{s_4, s_5\}$, $\{s_0, s_3\}$

2-equivalence classes: $\{s_1\}$, $\{s_2\}$, $\{s_4, s_5\}$, $\{s_0, s_3\}$

3-equivalence classes: $\{s_1\}$, $\{s_2\}$, $\{s_4, s_5\}$, $\{s_0, s_3\}$

Therefore, the states of $\overline{A}$ are the 3-equivalence classes of A.

For A':

0-equivalence classes: $\{s'_2, s'_3, s'_4, s'_5\}$, $\{s'_0, s'_1\}$

1-equivalence classes: $\{s'_2, s'_3, s'_4, s'_5\}$, $\{s'_0, s'_1\}$

Therefore, the states of $\overline{A'}$ are the 1-equivalence classes of A'.

According to the text, two automata are equivalent if, and only if, their quotient automata are isomorphic, provided inaccessible states have first been removed. Now A and A' have no inaccessible states, and $\overline{A}$ has four states, whereas $\overline{A'}$ has only two states. Therefore, A and A' are not equivalent.

This result can also be obtained by noting, for example, that the string 11 is accepted by A' but not by A.

11. *Partial answer:* Suppose A is a finite-state automaton with set of states S and relation R_* of $*$-equivalence of states. *[To show that R_* is an equivalence relation, we must show that R is reflexive, symmetric, and transitive.]*

Proof that R_* is symmetric:
[We must show that for all states s and t, if $s\ R_*\ t$ then $t\ R_*\ s$.] Suppose that s and t are any states of A such that $s\ R_*\ t$. *[We must show that $t\ R_*\ s$.]* Since $s\ R_*\ t$, then for every input string w,

$$\begin{bmatrix} N^*(s, w) \text{ is an} \\ \text{accepting state} \end{bmatrix} \Leftrightarrow \begin{bmatrix} N^*(t, w) \text{ is an} \\ \text{accepting state} \end{bmatrix},$$

where N^* is the eventual-state function on A. It follows from the symmetry of the $\Leftrightarrow$ relation that for every input string w,

$$\begin{bmatrix} N^*(t, w) \text{ is an} \\ \text{accepting state} \end{bmatrix} \Leftrightarrow \begin{bmatrix} N^*(s, w) \text{ is an} \\ \text{accepting state} \end{bmatrix}.$$

Hence $t\ R_*\ s$ *[as was to be shown]*, and so R_* is symmetric.

12. The proof is identical to the proof of property (12.3.1) given in the solution to exercise 11 provided every occurrence of "for each input string w" is replaced by "for each input string w of length less than or equal to k."

13. Proof: By property (12.3.2), for each integer $k \geq 0$, k-equivalence is an equivalence relation. Now by Theorem 10.3.4, the distinct equivalence classes of an equivalence relation form a partition of the set on which the relation is defined. In this case, the relation is defined on the set of all states of the automaton. So the k-equivalence classes form a partition of the set of all states of the automaton.

15. *Hint 1:* Suppose C_k is a particular but arbitrarily chosen k-equivalence class. You must show that there is a $(k-1)$-equivalence class C_{k-1} such that $C_k \subseteq C_{k-1}$.

Hint 2: If s is any element in C_k, then s is a state of the automaton. Now the $(k-1)$-equivalence classes partition the set of all states of the automaton into a union of mutually disjoint subsets, so $s \in C_{k-1}$ for *some* $(k-1)$-equivalence class C_{k-1}.

Hint 3: To show that $C_k \subseteq C_{k-1}$, you must show that for any state t, if $t \in C_k$, then $t \in C_{k-1}$.

17. *Hint:* If $m < k$, then every input string of length less than or equal to m has length less than or equal to k.

19. *Hint:* Suppose two states s and t are equivalent. You must show that for any input symbol m, the next-states $N(s, m)$ and $N(t, m)$ are equivalent. To do this, use the definition of equivalence and the fact that for any string w', input symbol m, and state s, $N^*(N(s, m), w') = N^*(s, mw')$.

INDEX