

**TABLE 9** Table for the Bit Operators *OR*, *AND*, and *XOR*.

$x$	$y$	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Information is often represented using bit strings, which are lists of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

### DEFINITION 7

A *bit string* is a sequence of zero or more bits. The *length* of this string is the number of bits in the string.

**EXAMPLE 12** 101010011 is a bit string of length nine.

We can extend bit operations to bit strings. We define the **bitwise OR**, **bitwise AND**, and **bitwise XOR** of two strings of the same length to be the strings that have as their bits the *OR*, *AND*, and *XOR* of the corresponding bits in the two strings, respectively. We use the symbols  $\vee$ ,  $\wedge$ , and  $\oplus$  to represent the bitwise *OR*, bitwise *AND*, and bitwise *XOR* operations, respectively. We illustrate bitwise operations on bit strings with Example 13.

**EXAMPLE 13** Find the bitwise *OR*, bitwise *AND*, and bitwise *XOR* of the bit strings 01 1011 0110 and 11 0001 1101. (Here, and throughout this book, bit strings will be split into blocks of four bits to make them easier to read.)

**Solution:** The bitwise *OR*, bitwise *AND*, and bitwise *XOR* of these strings are obtained by taking the *OR*, *AND*, and *XOR* of the corresponding bits, respectively. This gives us

```

01 1011 0110
11 0001 1101
-----
11 1011 1111    bitwise OR
01 0001 0100    bitwise AND
10 1010 1011    bitwise XOR

```

## Exercises

1. Which of these sentences are propositions? What are the truth values of those that are propositions?
  - a) Boston is the capital of Massachusetts.
  - b) Miami is the capital of Florida.
  - c)  $2 + 3 = 5$ .
  - d)  $5 + 7 = 10$ .
  - e)  $x + 2 = 11$ .
  - f) Answer this question.
2. Which of these are propositions? What are the truth values of those that are propositions?
  - a) Do not pass go.
  - b) What time is it?
  - c) There are no black flies in Maine.
  - d)  $4 + x = 5$ .
  - e) The moon is made of green cheese.
  - f)  $2^n \geq 100$ .
3. What is the negation of each of these propositions?
  - a) Mei has an MP3 player.
  - b) There is no pollution in New Jersey.
  - c)  $2 + 1 = 3$ .
  - d) The summer in Maine is hot and sunny.
4. What is the negation of each of these propositions?
  - a) Jennifer and Teja are friends.
  - b) There are 13 items in a baker's dozen.
  - c) Abby sent more than 100 text messages every day.
  - d) 121 is a perfect square.

5. What is the negation of each of these propositions?

- a) Steve has more than 100 GB free disk space on his laptop.
- b) Zach blocks e-mails and texts from Jennifer.
- c)  $7 \cdot 11 \cdot 13 = 999$ .
- d) Diane rode her bicycle 100 miles on Sunday.

6. Suppose that Smartphone A has 256 MB RAM and 32 GB ROM, and the resolution of its camera is 8 MP; Smartphone B has 288 MB RAM and 64 GB ROM, and the resolution of its camera is 4 MP; and Smartphone C has 128 MB RAM and 32 GB ROM, and the resolution of its camera is 5 MP. Determine the truth value of each of these propositions.

- a) Smartphone B has the most RAM of these three smartphones.
- b) Smartphone C has more ROM or a higher resolution camera than Smartphone B.
- c) Smartphone B has more RAM, more ROM, and a higher resolution camera than Smartphone A.
- d) If Smartphone B has more RAM and more ROM than Smartphone C, then it also has a higher resolution camera.
- e) Smartphone A has more RAM than Smartphone B if and only if Smartphone B has more RAM than Smartphone A.

7. Suppose that during the most recent fiscal year, the annual revenue of Acme Computer was 138 billion dollars and its net profit was 8 billion dollars, the annual revenue of Nadir Software was 87 billion dollars and its net profit was 5 billion dollars, and the annual revenue of Quixote Media was 111 billion dollars and its net profit was 13 billion dollars. Determine the truth value of each of these propositions for the most recent fiscal year.

- a) Quixote Media had the largest annual revenue.
- b) Nadir Software had the lowest net profit and Acme Computer had the largest annual revenue.
- c) Acme Computer had the largest net profit or Quixote Media had the largest net profit.
- d) If Quixote Media had the smallest net profit, then Acme Computer had the largest annual revenue.
- e) Nadir Software had the smallest net profit if and only if Acme Computer had the largest annual revenue.

8. Let  $p$  and  $q$  be the propositions

$p$  : I bought a lottery ticket this week.

$q$  : I won the million dollar jackpot.

Express each of these propositions as an English sentence.

- a)  $\neg p$
- b)  $p \vee q$
- c)  $p \rightarrow q$
- d)  $p \wedge q$
- e)  $p \leftrightarrow q$
- f)  $\neg p \rightarrow \neg q$
- g)  $\neg p \wedge \neg q$
- h)  $\neg p \vee (p \wedge q)$

9. Let  $p$  and  $q$  be the propositions “Swimming at the New Jersey shore is allowed” and “Sharks have been spotted near the shore,” respectively. Express each of these compound propositions as an English sentence.

- a)  $\neg q$
- b)  $p \wedge q$
- c)  $\neg p \vee q$
- d)  $p \rightarrow \neg q$
- e)  $\neg q \rightarrow p$
- f)  $\neg p \rightarrow \neg q$
- g)  $p \leftrightarrow \neg q$
- h)  $\neg p \wedge (p \vee \neg q)$

10. Let  $p$  and  $q$  be the propositions “The election is decided” and “The votes have been counted,” respectively. Express each of these compound propositions as an English sentence.

- a)  $\neg p$
- b)  $p \vee q$
- c)  $\neg p \wedge q$
- d)  $q \rightarrow p$
- e)  $\neg q \rightarrow \neg p$
- f)  $\neg p \rightarrow \neg q$
- g)  $p \leftrightarrow q$
- h)  $\neg q \vee (\neg p \wedge q)$

11. Let  $p$  and  $q$  be the propositions

$p$  : It is below freezing.

$q$  : It is snowing.

Write these propositions using  $p$  and  $q$  and logical connectives (including negations).

- a) It is below freezing and snowing.
- b) It is below freezing but not snowing.
- c) It is not below freezing and it is not snowing.
- d) It is either snowing or below freezing (or both).
- e) If it is below freezing, it is also snowing.
- f) Either it is below freezing or it is snowing, but it is not snowing if it is below freezing.
- g) That it is below freezing is necessary and sufficient for it to be snowing.

12. Let  $p$ ,  $q$ , and  $r$  be the propositions

$p$  : You have the flu.

$q$  : You miss the final examination.

$r$  : You pass the course.

Express each of these propositions as an English sentence.

- a)  $p \rightarrow q$
- b)  $\neg q \leftrightarrow r$
- c)  $q \rightarrow \neg r$
- d)  $p \vee q \vee r$
- e)  $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$
- f)  $(p \wedge q) \vee (\neg q \wedge r)$

13. Let  $p$  and  $q$  be the propositions

$p$  : You drive over 65 miles per hour.

$q$  : You get a speeding ticket.

Write these propositions using  $p$  and  $q$  and logical connectives (including negations).

- a) You do not drive over 65 miles per hour.
- b) You drive over 65 miles per hour, but you do not get a speeding ticket.
- c) You will get a speeding ticket if you drive over 65 miles per hour.
- d) If you do not drive over 65 miles per hour, then you will not get a speeding ticket.
- e) Driving over 65 miles per hour is sufficient for getting a speeding ticket.
- f) You get a speeding ticket, but you do not drive over 65 miles per hour.
- g) Whenever you get a speeding ticket, you are driving over 65 miles per hour.

14. Let  $p$ ,  $q$ , and  $r$  be the propositions

$p$  : You get an A on the final exam.

$q$  : You do every exercise in this book.

$r$  : You get an A in this class.

Write these propositions using  $p$ ,  $q$ , and  $r$  and logical connectives (including negations).

- a) You get an A in this class, but you do not do every exercise in this book.
  - b) You get an A on the final, you do every exercise in this book, and you get an A in this class.
  - c) To get an A in this class, it is necessary for you to get an A on the final.
  - d) You get an A on the final, but you don't do every exercise in this book; nevertheless, you get an A in this class.
  - e) Getting an A on the final and doing every exercise in this book is sufficient for getting an A in this class.
  - f) You will get an A in this class if and only if you either do every exercise in this book or you get an A on the final.
15. Let  $p$ ,  $q$ , and  $r$  be the propositions
- $p$  : Grizzly bears have been seen in the area.  
 $q$  : Hiking is safe on the trail.  
 $r$  : Berries are ripe along the trail.
- Write these propositions using  $p$ ,  $q$ , and  $r$  and logical connectives (including negations).
- a) Berries are ripe along the trail, but grizzly bears have not been seen in the area.
  - b) Grizzly bears have not been seen in the area and hiking on the trail is safe, but berries are ripe along the trail.
  - c) If berries are ripe along the trail, hiking is safe if and only if grizzly bears have not been seen in the area.
  - d) It is not safe to hike on the trail, but grizzly bears have not been seen in the area and the berries along the trail are ripe.
  - e) For hiking on the trail to be safe, it is necessary but not sufficient that berries not be ripe along the trail and for grizzly bears not to have been seen in the area.
  - f) Hiking is not safe on the trail whenever grizzly bears have been seen in the area and berries are ripe along the trail.
16. Determine whether these biconditionals are true or false.
- a)  $2 + 2 = 4$  if and only if  $1 + 1 = 2$ .
  - b)  $1 + 1 = 2$  if and only if  $2 + 3 = 4$ .
  - c)  $1 + 1 = 3$  if and only if monkeys can fly.
  - d)  $0 > 1$  if and only if  $2 > 1$ .
17. Determine whether each of these conditional statements is true or false.
- a) If  $1 + 1 = 2$ , then  $2 + 2 = 5$ .
  - b) If  $1 + 1 = 3$ , then  $2 + 2 = 4$ .
  - c) If  $1 + 1 = 3$ , then  $2 + 2 = 5$ .
  - d) If monkeys can fly, then  $1 + 1 = 3$ .
18. Determine whether each of these conditional statements is true or false.
- a) If  $1 + 1 = 3$ , then unicorns exist.
  - b) If  $1 + 1 = 3$ , then dogs can fly.
  - c) If  $1 + 1 = 2$ , then dogs can fly.
  - d) If  $2 + 2 = 4$ , then  $1 + 2 = 3$ .
19. For each of these sentences, determine whether an inclusive or, or an exclusive or, is intended. Explain your answer.
- a) Coffee or tea comes with dinner.
  - b) A password must have at least three digits or be at least eight characters long.
  - c) The prerequisite for the course is a course in number theory or a course in cryptography.
  - d) You can pay using U.S. dollars or euros.
20. For each of these sentences, determine whether an inclusive or, or an exclusive or, is intended. Explain your answer.
- a) Experience with C++ or Java is required.
  - b) Lunch includes soup or salad.
  - c) To enter the country you need a passport or a voter registration card.
  - d) Publish or perish.
21. For each of these sentences, state what the sentence means if the logical connective or is an inclusive or (that is, a disjunction) versus an exclusive or. Which of these meanings of or do you think is intended?
- a) To take discrete mathematics, you must have taken calculus or a course in computer science.
  - b) When you buy a new car from Acme Motor Company, you get \$2000 back in cash or a 2% car loan.
  - c) Dinner for two includes two items from column A or three items from column B.
  - d) School is closed if more than 2 feet of snow falls or if the wind chill is below  $-100$ .
22. Write each of these statements in the form "if  $p$ , then  $q$ " in English. [*Hint*: Refer to the list of common ways to express conditional statements provided in this section.]
- a) It is necessary to wash the boss's car to get promoted.
  - b) Winds from the south imply a spring thaw.
  - c) A sufficient condition for the warranty to be good is that you bought the computer less than a year ago.
  - d) Willy gets caught whenever he cheats.
  - e) You can access the website only if you pay a subscription fee.
  - f) Getting elected follows from knowing the right people.
  - g) Carol gets seasick whenever she is on a boat.
23. Write each of these statements in the form "if  $p$ , then  $q$ " in English. [*Hint*: Refer to the list of common ways to express conditional statements.]
- a) It snows whenever the wind blows from the northeast.
  - b) The apple trees will bloom if it stays warm for a week.
  - c) That the Pistons win the championship implies that they beat the Lakers.
  - d) It is necessary to walk 8 miles to get to the top of Long's Peak.
  - e) To get tenure as a professor, it is sufficient to be world-famous.
  - f) If you drive more than 400 miles, you will need to buy gasoline.
  - g) Your guarantee is good only if you bought your CD player less than 90 days ago.
  - h) Jan will go swimming unless the water is too cold.

24. Write each of these statements in the form “if  $p$ , then  $q$ ” in English. [*Hint*: Refer to the list of common ways to express conditional statements provided in this section.]
- I will remember to send you the address only if you send me an e-mail message.
  - To be a citizen of this country, it is sufficient that you were born in the United States.
  - If you keep your textbook, it will be a useful reference in your future courses.
  - The Red Wings will win the Stanley Cup if their goalie plays well.
  - That you get the job implies that you had the best credentials.
  - The beach erodes whenever there is a storm.
  - It is necessary to have a valid password to log on to the server.
  - You will reach the summit unless you begin your climb too late.
25. Write each of these propositions in the form “ $p$  if and only if  $q$ ” in English.
- If it is hot outside you buy an ice cream cone, and if you buy an ice cream cone it is hot outside.
  - For you to win the contest it is necessary and sufficient that you have the only winning ticket.
  - You get promoted only if you have connections, and you have connections only if you get promoted.
  - If you watch television your mind will decay, and conversely.
  - The trains run late on exactly those days when I take it.
26. Write each of these propositions in the form “ $p$  if and only if  $q$ ” in English.
- For you to get an A in this course, it is necessary and sufficient that you learn how to solve discrete mathematics problems.
  - If you read the newspaper every day, you will be informed, and conversely.
  - It rains if it is a weekend day, and it is a weekend day if it rains.
  - You can see the wizard only if the wizard is not in, and the wizard is not in only if you can see him.
27. State the converse, contrapositive, and inverse of each of these conditional statements.
- If it snows today, I will ski tomorrow.
  - I come to class whenever there is going to be a quiz.
  - A positive integer is a prime only if it has no divisors other than 1 and itself.
28. State the converse, contrapositive, and inverse of each of these conditional statements.
- If it snows tonight, then I will stay at home.
  - I go to the beach whenever it is a sunny summer day.
  - When I stay up late, it is necessary that I sleep until noon.
29. How many rows appear in a truth table for each of these compound propositions?
- $p \rightarrow \neg p$
  - $(p \vee \neg r) \wedge (q \vee \neg s)$
  - $q \vee p \vee \neg s \vee \neg r \vee \neg t \vee u$
  - $(p \wedge r \wedge t) \leftrightarrow (q \wedge t)$
30. How many rows appear in a truth table for each of these compound propositions?
- $(q \rightarrow \neg p) \vee (\neg p \rightarrow \neg q)$
  - $(p \vee \neg t) \wedge (p \vee \neg s)$
  - $(p \rightarrow r) \vee (\neg s \rightarrow \neg t) \vee (\neg u \rightarrow v)$
  - $(p \wedge r \wedge s) \vee (q \wedge t) \vee (r \wedge \neg t)$
31. Construct a truth table for each of these compound propositions.
- $p \wedge \neg p$
  - $p \vee \neg p$
  - $(p \vee \neg q) \rightarrow q$
  - $(p \vee q) \rightarrow (p \wedge q)$
  - $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
  - $(p \rightarrow q) \rightarrow (q \rightarrow p)$
32. Construct a truth table for each of these compound propositions.
- $p \rightarrow \neg p$
  - $p \leftrightarrow \neg p$
  - $p \oplus (p \vee q)$
  - $(p \wedge q) \rightarrow (p \vee q)$
  - $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$
  - $(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$
33. Construct a truth table for each of these compound propositions.
- $(p \vee q) \rightarrow (p \oplus q)$
  - $(p \oplus q) \rightarrow (p \wedge q)$
  - $(p \vee q) \oplus (p \wedge q)$
  - $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$
  - $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$
  - $(p \oplus q) \rightarrow (p \oplus \neg q)$
34. Construct a truth table for each of these compound propositions.
- $p \oplus p$
  - $p \oplus \neg p$
  - $p \oplus \neg q$
  - $\neg p \oplus \neg q$
  - $(p \oplus q) \vee (p \oplus \neg q)$
  - $(p \oplus q) \wedge (p \oplus \neg q)$
35. Construct a truth table for each of these compound propositions.
- $p \rightarrow \neg q$
  - $\neg p \leftrightarrow q$
  - $(p \rightarrow q) \vee (\neg p \rightarrow q)$
  - $(p \rightarrow q) \wedge (\neg p \rightarrow q)$
  - $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$
  - $(\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q)$
36. Construct a truth table for each of these compound propositions.
- $(p \vee q) \vee r$
  - $(p \vee q) \wedge r$
  - $(p \wedge q) \vee r$
  - $(p \wedge q) \wedge r$
  - $(p \vee q) \wedge \neg r$
  - $(p \wedge q) \vee \neg r$
37. Construct a truth table for each of these compound propositions.
- $p \rightarrow (\neg q \vee r)$
  - $\neg p \rightarrow (q \rightarrow r)$
  - $(p \rightarrow q) \vee (\neg p \rightarrow r)$
  - $(p \rightarrow q) \wedge (\neg p \rightarrow r)$
  - $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$
  - $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$
38. Construct a truth table for  $((p \rightarrow q) \rightarrow r) \rightarrow s$ .
39. Construct a truth table for  $(p \leftrightarrow q) \leftrightarrow (r \leftrightarrow s)$ .

40. Explain, without using a truth table, why  $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$  is true when  $p$ ,  $q$ , and  $r$  have the same truth value and it is false otherwise.
41. Explain, without using a truth table, why  $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$  is true when at least one of  $p$ ,  $q$ , and  $r$  is true and at least one is false, but is false when all three variables have the same truth value.
42. What is the value of  $x$  after each of these statements is encountered in a computer program, if  $x = 1$  before the statement is reached?
- if  $x + 2 = 3$  then  $x := x + 1$
  - if  $(x + 1 = 3)$  OR  $(2x + 2 = 3)$  then  $x := x + 1$
  - if  $(2x + 3 = 5)$  AND  $(3x + 4 = 7)$  then  $x := x + 1$
  - if  $(x + 1 = 2)$  XOR  $(x + 2 = 3)$  then  $x := x + 1$
  - if  $x < 2$  then  $x := x + 1$
43. Find the bitwise OR, bitwise AND, and bitwise XOR of each of these pairs of bit strings.
- 101 1110, 010 0001
  - 1111 0000, 1010 1010
  - 00 0111 0001, 10 0100 1000
  - 11 1111 1111, 00 0000 0000
44. Evaluate each of these expressions.
- $1\ 1000 \wedge (0\ 1011 \vee 1\ 1011)$
  - $(0\ 1111 \wedge 1\ 0101) \vee 0\ 1000$
  - $(0\ 1010 \oplus 1\ 1011) \oplus 0\ 1000$
  - $(1\ 1011 \vee 0\ 1010) \wedge (1\ 0001 \vee 1\ 1011)$
- Fuzzy logic** is used in artificial intelligence. In fuzzy logic, a proposition has a truth value that is a number between 0 and 1, inclusive. A proposition with a truth value of 0 is false and one with a truth value of 1 is true. Truth values that are between 0 and 1 indicate varying degrees of truth. For instance, the truth value 0.8 can be assigned to the statement “Fred is happy,” because Fred is happy most of the time, and the truth value 0.4 can be assigned to the statement “John is happy,” because John is happy slightly less than half the time. Use these truth values to solve Exercises 45–47.
45. The truth value of the negation of a proposition in fuzzy logic is 1 minus the truth value of the proposition. What are the truth values of the statements “Fred is not happy” and “John is not happy?”
46. The truth value of the conjunction of two propositions in fuzzy logic is the minimum of the truth values of the two propositions. What are the truth values of the statements “Fred and John are happy” and “Neither Fred nor John is happy?”
47. The truth value of the disjunction of two propositions in fuzzy logic is the maximum of the truth values of the two propositions. What are the truth values of the statements “Fred is happy, or John is happy” and “Fred is not happy, or John is not happy?”
- \*48. Is the assertion “This statement is false” a proposition?
- \*49. The  $n$ th statement in a list of 100 statements is “Exactly  $n$  of the statements in this list are false.”
- What conclusions can you draw from these statements?
  - Answer part (a) if the  $n$ th statement is “At least  $n$  of the statements in this list are false.”
  - Answer part (b) assuming that the list contains 99 statements.
50. An ancient Sicilian legend says that the barber in a remote town who can be reached only by traveling a dangerous mountain road shaves those people, and only those people, who do not shave themselves. Can there be such a barber?

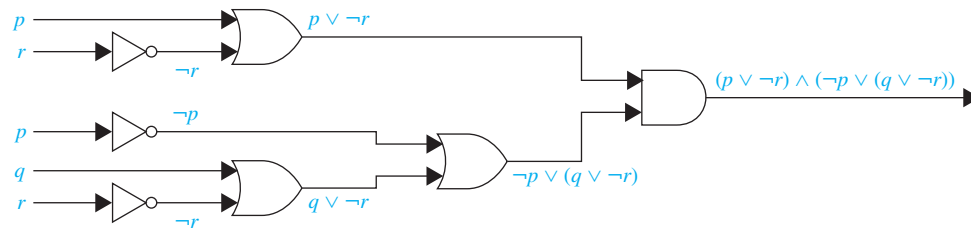
## 1.2 Applications of Propositional Logic

### Introduction

Logic has many important applications to mathematics, computer science, and numerous other disciplines. Statements in mathematics and the sciences and in natural language often are imprecise or ambiguous. To make such statements precise, they can be translated into the language of logic. For example, logic is used in the specification of software and hardware, because these specifications need to be precise before development begins. Furthermore, propositional logic and its rules can be used to design computer circuits, to construct computer programs, to verify the correctness of programs, and to build expert systems. Logic can be used to analyze and solve many familiar puzzles. Software systems based on the rules of logic have been developed for constructing some, but not all, types of proofs automatically. We will discuss some of these applications of propositional logic in this section and in later chapters.

### Translating English Sentences

There are many reasons to translate English sentences into expressions involving propositional variables and logical connectives. In particular, English (and every other human language) is



**FIGURE 3** The circuit for  $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$ .

## Exercises

In Exercises 1–6, translate the given statement into propositional logic using the propositions provided.

1. You cannot edit a protected Wikipedia entry unless you are an administrator. Express your answer in terms of  $e$ : “You can edit a protected Wikipedia entry” and  $a$ : “You are an administrator.”
2. You can see the movie only if you are over 18 years old or you have the permission of a parent. Express your answer in terms of  $m$ : “You can see the movie,”  $e$ : “You are over 18 years old,” and  $p$ : “You have the permission of a parent.”
3. You can graduate only if you have completed the requirements of your major and you do not owe money to the university and you do not have an overdue library book. Express your answer in terms of  $g$ : “You can graduate,”  $m$ : “You owe money to the university,”  $r$ : “You have completed the requirements of your major,” and  $b$ : “You have an overdue library book.”
4. To use the wireless network in the airport you must pay the daily fee unless you are a subscriber to the service. Express your answer in terms of  $w$ : “You can use the wireless network in the airport,”  $d$ : “You pay the daily fee,” and  $s$ : “You are a subscriber to the service.”
5. You are eligible to be President of the U.S.A. only if you are at least 35 years old, were born in the U.S.A., or at the time of your birth both of your parents were citizens, and you have lived at least 14 years in the country. Express your answer in terms of  $e$ : “You are eligible to be President of the U.S.A.,”  $a$ : “You are at least 35 years old,”  $b$ : “You were born in the U.S.A.,”  $p$ : “At the time of your birth, both of your parents were citizens,” and  $r$ : “You have lived at least 14 years in the U.S.A.”
6. You can upgrade your operating system only if you have a 32-bit processor running at 1 GHz or faster, at least 1 GB RAM, and 16 GB free hard disk space, or a 64-bit processor running at 2 GHz or faster, at least 2 GB RAM, and at least 32 GB free hard disk space. Express your answer in terms of  $u$ : “You can upgrade your operating system,”  $b_{32}$ : “You have a 32-bit processor,”  $b_{64}$ :


“You have a 64-bit processor,”  $g_1$ : “Your processor runs at 1 GHz or faster,”  $g_2$ : “Your processor runs at 2 GHz or faster,”  $r_1$ : “Your processor has at least 1 GB RAM,”  $r_2$ : “Your processor has at least 2 GB RAM,”  $h_{16}$ : “You have at least 16 GB free hard disk space,” and  $h_{32}$ : “You have at least 32 GB free hard disk space.”

7. Express these system specifications using the propositions  $p$  “The message is scanned for viruses” and  $q$  “The message was sent from an unknown system” together with logical connectives (including negations).
  - a) “The message is scanned for viruses whenever the message was sent from an unknown system.”
  - b) “The message was sent from an unknown system but it was not scanned for viruses.”
  - c) “It is necessary to scan the message for viruses whenever it was sent from an unknown system.”
  - d) “When a message is not sent from an unknown system it is not scanned for viruses.”
8. Express these system specifications using the propositions  $p$  “The user enters a valid password,”  $q$  “Access is granted,” and  $r$  “The user has paid the subscription fee” and logical connectives (including negations).
  - a) “The user has paid the subscription fee, but does not enter a valid password.”
  - b) “Access is granted whenever the user has paid the subscription fee and enters a valid password.”
  - c) “Access is denied if the user has not paid the subscription fee.”
  - d) “If the user has not entered a valid password but has paid the subscription fee, then access is granted.”
9. Are these system specifications consistent? “The system is in multiuser state if and only if it is operating normally. If the system is operating normally, the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt mode. The system is not in interrupt mode.”

10. Are these system specifications consistent? “Whenever the system software is being upgraded, users cannot access the file system. If users can access the file system, then they can save new files. If users cannot save new files, then the system software is not being upgraded.”
  11. Are these system specifications consistent? “The router can send packets to the edge system only if it supports the new address space. For the router to support the new address space it is necessary that the latest software release be installed. The router can send packets to the edge system if the latest software release is installed, The router does not support the new address space.”
  12. Are these system specifications consistent? “If the file system is not locked, then new messages will be queued. If the file system is not locked, then the system is functioning normally, and conversely. If new messages are not queued, then they will be sent to the message buffer. If the file system is not locked, then new messages will be sent to the message buffer. New messages will not be sent to the message buffer.”
  13. What Boolean search would you use to look for Web pages about beaches in New Jersey? What if you wanted to find Web pages about beaches on the isle of Jersey (in the English Channel)?
  14. What Boolean search would you use to look for Web pages about hiking in West Virginia? What if you wanted to find Web pages about hiking in Virginia, but not in West Virginia?
  - \*15. Each inhabitant of a remote village always tells the truth or always lies. A villager will give only a “Yes” or a “No” response to a question a tourist asks. Suppose you are a tourist visiting this area and come to a fork in the road. One branch leads to the ruins you want to visit; the other branch leads deep into the jungle. A villager is standing at the fork in the road. What one question can you ask the villager to determine which branch to take?
  16. An explorer is captured by a group of cannibals. There are two types of cannibals—those who always tell the truth and those who always lie. The cannibals will barbecue the explorer unless he can determine whether a particular cannibal always lies or always tells the truth. He is allowed to ask the cannibal exactly one question.
    - a) Explain why the question “Are you a liar?” does not work.
    - b) Find a question that the explorer can use to determine whether the cannibal always lies or always tells the truth.
  17. When three professors are seated in a restaurant, the hostess asks them: “Does everyone want coffee?” The first professor says: “I do not know.” The second professor then says: “I do not know.” Finally, the third professor says: “No, not everyone wants coffee.” The hostess comes back and gives coffee to the professors who want it. How did she figure out who wanted coffee?
  18. When planning a party you want to know whom to invite. Among the people you would like to invite are three touchy friends. You know that if Jasmine attends, she will become unhappy if Samir is there, Samir will attend only if Kanti will be there, and Kanti will not attend unless Jasmine also does. Which combinations of these three friends can you invite so as not to make someone unhappy?
- Exercises 19–23 relate to inhabitants of the island of knights and knaves created by Smullyan, where knights always tell the truth and knaves always lie. You encounter two people, *A* and *B*. Determine, if possible, what *A* and *B* are if they address you in the ways described. If you cannot determine what these two people are, can you draw any conclusions?
19. *A* says “At least one of us is a knave” and *B* says nothing.
  20. *A* says “The two of us are both knights” and *B* says “*A* is a knave.”
  21. *A* says “I am a knave or *B* is a knight” and *B* says nothing.
  22. Both *A* and *B* say “I am a knight.”
  23. *A* says “We are both knaves” and *B* says nothing.
- Exercises 24–31 relate to inhabitants of an island on which there are three kinds of people: knights who always tell the truth, knaves who always lie, and spies (called normals by Smullyan [Sm78]) who can either lie or tell the truth. You encounter three people, *A*, *B*, and *C*. You know one of these people is a knight, one is a knave, and one is a spy. Each of the three people knows the type of person each of other two is. For each of these situations, if possible, determine whether there is a unique solution and determine who the knave, knight, and spy are. When there is no unique solution, list all possible solutions or state that there are no solutions.
24. *A* says “*C* is the knave,” *B* says, “*A* is the knight,” and *C* says “I am the spy.”
  25. *A* says “I am the knight,” *B* says “I am the knave,” and *C* says “*B* is the knight.”
  26. *A* says “I am the knave,” *B* says “I am the knave,” and *C* says “I am the knave.”
  27. *A* says “I am the knight,” *B* says “*A* is telling the truth,” and *C* says “I am the spy.”
  28. *A* says “I am the knight,” *B* says, “*A* is not the knave,” and *C* says “*B* is not the knave.”
  29. *A* says “I am the knight,” *B* says “I am the knight,” and *C* says “I am the knight.”
  30. *A* says “I am not the spy,” *B* says “I am not the spy,” and *C* says “*A* is the spy.”
  31. *A* says “I am not the spy,” *B* says “I am not the spy,” and *C* says “I am not the spy.”
- Exercises 32–38 are puzzles that can be solved by translating statements into logical expressions and reasoning from these expressions using truth tables.
32. The police have three suspects for the murder of Mr. Cooper: Mr. Smith, Mr. Jones, and Mr. Williams. Smith, Jones, and Williams each declare that they did not kill Cooper. Smith also states that Cooper was a friend of Jones and that Williams disliked him. Jones also states that he did not know Cooper and that he was out of town the day Cooper was killed. Williams also states that he

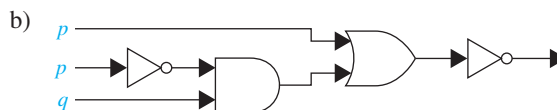
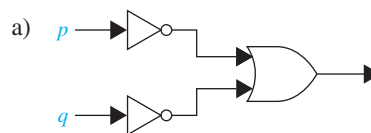
saw both Smith and Jones with Cooper the day of the killing and that either Smith or Jones must have killed him. Can you determine who the murderer was if

- one of the three men is guilty, the two innocent men are telling the truth, but the statements of the guilty man may or may not be true?
- innocent men do not lie?

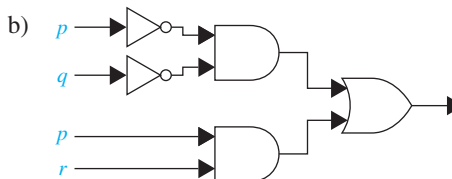
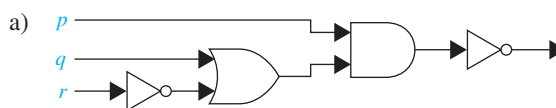
- Steve would like to determine the relative salaries of three coworkers using two facts. First, he knows that if Fred is not the highest paid of the three, then Janice is. Second, he knows that if Janice is not the lowest paid, then Maggie is paid the most. Is it possible to determine the relative salaries of Fred, Maggie, and Janice from what Steve knows? If so, who is paid the most and who the least? Explain your reasoning.
- Five friends have access to a chat room. Is it possible to determine who is chatting if the following information is known? Either Kevin or Heather, or both, are chatting. Either Randy or Vijay, but not both, are chatting. If Abby is chatting, so is Randy. Vijay and Kevin are either both chatting or neither is. If Heather is chatting, then so are Abby and Kevin. Explain your reasoning.
- A detective has interviewed four witnesses to a crime. From the stories of the witnesses the detective has concluded that if the butler is telling the truth then so is the cook; the cook and the gardener cannot both be telling the truth; the gardener and the handyman are not both lying; and if the handyman is telling the truth then the cook is lying. For each of the four witnesses, can the detective determine whether that person is telling the truth or lying? Explain your reasoning.
- Four friends have been identified as suspects for an unauthorized access into a computer system. They have made statements to the investigating authorities. Alice said “Carlos did it.” John said “I did not do it.” Carlos said “Diana did it.” Diana said “Carlos lied when he said that I did it.”
  - If the authorities also know that exactly one of the four suspects is telling the truth, who did it? Explain your reasoning.
  - If the authorities also know that exactly one is lying, who did it? Explain your reasoning.
- Suppose there are signs on the doors to two rooms. The sign on the first door reads “In this room there is a lady, and in the other one there is a tiger”; and the sign on the second door reads “In one of these rooms, there is a lady, and in one of them there is a tiger.” Suppose that you know that one of these signs is true and the other is false. Behind which door is the lady?
-  Solve this famous logic puzzle, attributed to Albert Einstein, and known as the **zebra puzzle**. Five men with different nationalities and with different jobs live in consecutive houses on a street. These houses are painted different colors. The men have different pets and have different favorite drinks. Determine who owns a zebra and

whose favorite drink is mineral water (which is one of the favorite drinks) given these clues: The Englishman lives in the red house. The Spaniard owns a dog. The Japanese man is a painter. The Italian drinks tea. The Norwegian lives in the first house on the left. The green house is immediately to the right of the white one. The photographer breeds snails. The diplomat lives in the yellow house. Milk is drunk in the middle house. The owner of the green house drinks coffee. The Norwegian’s house is next to the blue one. The violinist drinks orange juice. The fox is in a house next to that of the physician. The horse is in a house next to that of the diplomat. [Hint: Make a table where the rows represent the men and columns represent the color of their houses, their jobs, their pets, and their favorite drinks and use logical reasoning to determine the correct entries in the table.]

- Freedonia has fifty senators. Each senator is either honest or corrupt. Suppose you know that at least one of the Freedonian senators is honest and that, given any two Freedonian senators, at least one is corrupt. Based on these facts, can you determine how many Freedonian senators are honest and how many are corrupt? If so, what is the answer?
- Find the output of each of these combinatorial circuits.



- Find the output of each of these combinatorial circuits.



- Construct a combinatorial circuit using inverters, OR gates, and AND gates that produces the output  $(p \wedge \neg r) \vee (\neg q \wedge r)$  from input bits  $p$ ,  $q$ , and  $r$ .
- Construct a combinatorial circuit using inverters, OR gates, and AND gates that produces the output  $((\neg p \vee \neg r) \wedge \neg q) \vee (\neg p \wedge (q \vee r))$  from input bits  $p$ ,  $q$ , and  $r$ .



## Solving Satisfiability Problems

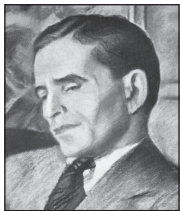
A truth table can be used to determine whether a compound proposition is satisfiable, or equivalently, whether its negation is a tautology (see Exercise 60). This can be done by hand for a compound proposition with a small number of variables, but when the number of variables grows, this becomes impractical. For instance, there are  $2^{20} = 1,048,576$  rows in the truth table for a compound proposition with 20 variables. Clearly, you need a computer to help you determine, in this way, whether a compound proposition in 20 variables is satisfiable.

When many applications are modeled, questions concerning the satisfiability of compound propositions with hundreds, thousands, or millions of variables arise. Note, for example, that when there are 1000 variables, checking every one of the  $2^{1000}$  (a number with more than 300 decimal digits) possible combinations of truth values of the variables in a compound proposition cannot be done by a computer in even trillions of years. No procedure is known that a computer can follow to determine in a reasonable amount of time whether an arbitrary compound proposition in such a large number of variables is satisfiable. However, progress has been made developing methods for solving the satisfiability problem for the particular types of compound propositions that arise in practical applications, such as for the solution of Sudoku puzzles. Many computer programs have been developed for solving satisfiability problems which have practical use. In our discussion of the subject of algorithms in Chapter 3, we will discuss this question further. In particular, we will explain the important role the propositional satisfiability problem plays in the study of the complexity of algorithms.



## Exercises

- Use truth tables to verify these equivalences.
  - $p \wedge \mathbf{T} \equiv p$
  - $p \vee \mathbf{F} \equiv p$
  - $p \wedge \mathbf{F} \equiv \mathbf{F}$
  - $p \vee \mathbf{T} \equiv \mathbf{T}$
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- Show that  $\neg(\neg p)$  and  $p$  are logically equivalent.
- Use truth tables to verify the commutative laws
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- Use truth tables to verify the associative laws
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- Use a truth table to verify the distributive law
 
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r).$$
- Use a truth table to verify the first De Morgan law
 
$$\neg(p \wedge q) \equiv \neg p \vee \neg q.$$
- Use De Morgan's laws to find the negation of each of the following statements.
  - Jan is rich and happy.
  - Carlos will bicycle or run tomorrow.




**HENRY MAURICE SHEFFER (1883–1964)** Henry Maurice Sheffer, born to Jewish parents in the western Ukraine, emigrated to the United States in 1892 with his parents and six siblings. He studied at the Boston Latin School before entering Harvard, where he completed his undergraduate degree in 1905, his master's in 1907, and his Ph.D. in philosophy in 1908. After holding a postdoctoral position at Harvard, Henry traveled to Europe on a fellowship. Upon returning to the United States, he became an academic nomad, spending one year each at the University of Washington, Cornell, the University of Minnesota, the University of Missouri, and City College in New York. In 1916 he returned to Harvard as a faculty member in the philosophy department. He remained at Harvard until his retirement in 1952.


Sheffer introduced what is now known as the Sheffer stroke in 1913; it became well known only after its use in the 1925 edition of Whitehead and Russell's *Principia Mathematica*. In this same edition Russell wrote that Sheffer had invented a powerful method that could be used to simplify the *Principia*. Because of this comment, Sheffer was something of a mystery man to logicians, especially because Sheffer, who published little in his career, never published the details of this method, only describing it in mimeographed notes and in a brief published abstract.

Sheffer was a dedicated teacher of mathematical logic. He liked his classes to be small and did not like auditors. When strangers appeared in his classroom, Sheffer would order them to leave, even his colleagues or distinguished guests visiting Harvard. Sheffer was barely five feet tall; he was noted for his wit and vigor, as well as for his nervousness and irritability. Although widely liked, he was quite lonely. He is noted for a quip he spoke at his retirement: "Old professors never die, they just become emeriti." Sheffer is also credited with coining the term "Boolean algebra" (the subject of Chapter 12 of this text). Sheffer was briefly married and lived most of his later life in small rooms at a hotel packed with his logic books and vast files of slips of paper he used to jot down his ideas. Unfortunately, Sheffer suffered from severe depression during the last two decades of his life.

- c) Mei walks or takes the bus to class.
  - d) Ibrahim is smart and hard working.
8. Use De Morgan's laws to find the negation of each of the following statements.
- a) Kwame will take a job in industry or go to graduate school.
  - b) Yoshiko knows Java and calculus.
  - c) James is young and strong.
  - d) Rita will move to Oregon or Washington.

 9. Show that each of these conditional statements is a tautology by using truth tables.

- a)  $(p \wedge q) \rightarrow p$
- b)  $p \rightarrow (p \vee q)$
- c)  $\neg p \rightarrow (p \rightarrow q)$
- d)  $(p \wedge q) \rightarrow (p \rightarrow q)$
- e)  $\neg(p \rightarrow q) \rightarrow p$
- f)  $\neg(p \rightarrow q) \rightarrow \neg q$

 10. Show that each of these conditional statements is a tautology by using truth tables.

- a)  $[\neg p \wedge (p \vee q)] \rightarrow q$
- b)  $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
- c)  $[p \wedge (p \rightarrow q)] \rightarrow q$
- d)  $[(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow r$


11. Show that each conditional statement in Exercise 9 is a tautology without using truth tables.

12. Show that each conditional statement in Exercise 10 is a tautology without using truth tables.

13. Use truth tables to verify the absorption laws.

- a)  $p \vee (p \wedge q) \equiv p$
- b)  $p \wedge (p \vee q) \equiv p$


14. Determine whether  $(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$  is a tautology.

 15. Determine whether  $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$  is a tautology.

Each of Exercises 16–28 asks you to show that two compound propositions are logically equivalent. To do this, either show that both sides are true, or that both sides are false, for exactly the same combinations of truth values of the propositional variables in these expressions (whichever is easier).

- 16. Show that  $p \leftrightarrow q$  and  $(p \wedge q) \vee (\neg p \wedge \neg q)$  are logically equivalent.
- 17. Show that  $\neg(p \leftrightarrow q)$  and  $p \leftrightarrow \neg q$  are logically equivalent.
- 18. Show that  $p \rightarrow q$  and  $\neg q \rightarrow \neg p$  are logically equivalent.
- 19. Show that  $\neg p \leftrightarrow q$  and  $p \leftrightarrow \neg q$  are logically equivalent.
- 20. Show that  $\neg(p \oplus q)$  and  $p \leftrightarrow q$  are logically equivalent.
- 21. Show that  $\neg(p \leftrightarrow q)$  and  $\neg p \leftrightarrow q$  are logically equivalent.
- 22. Show that  $(p \rightarrow q) \wedge (p \rightarrow r)$  and  $p \rightarrow (q \wedge r)$  are logically equivalent.
- 23. Show that  $(p \rightarrow r) \wedge (q \rightarrow r)$  and  $(p \vee q) \rightarrow r$  are logically equivalent.
- 24. Show that  $(p \rightarrow q) \vee (p \rightarrow r)$  and  $p \rightarrow (q \vee r)$  are logically equivalent.
- 25. Show that  $(p \rightarrow r) \vee (q \rightarrow r)$  and  $(p \wedge q) \rightarrow r$  are logically equivalent.
- 26. Show that  $\neg p \rightarrow (q \rightarrow r)$  and  $q \rightarrow (p \vee r)$  are logically equivalent.
- 27. Show that  $p \leftrightarrow q$  and  $(p \rightarrow q) \wedge (q \rightarrow p)$  are logically equivalent.
- 28. Show that  $p \leftrightarrow q$  and  $\neg p \leftrightarrow \neg q$  are logically equivalent.

29. Show that  $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$  is a tautology.

 30. Show that  $(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$  is a tautology.

31. Show that  $(p \rightarrow q) \rightarrow r$  and  $p \rightarrow (q \rightarrow r)$  are not logically equivalent.

32. Show that  $(p \wedge q) \rightarrow r$  and  $(p \rightarrow r) \wedge (q \rightarrow r)$  are not logically equivalent.

33. Show that  $(p \rightarrow q) \rightarrow (r \rightarrow s)$  and  $(p \rightarrow r) \rightarrow (q \rightarrow s)$  are not logically equivalent.

The **dual** of a compound proposition that contains only the logical operators  $\vee$ ,  $\wedge$ , and  $\neg$  is the compound proposition obtained by replacing each  $\vee$  by  $\wedge$ , each  $\wedge$  by  $\vee$ , each **T** by **F**, and each **F** by **T**. The dual of  $s$  is denoted by  $s^*$ .

34. Find the dual of each of these compound propositions.

- a)  $p \vee \neg q$
- b)  $p \wedge (q \vee (r \wedge \mathbf{T}))$
- c)  $(p \wedge \neg q) \vee (q \wedge \mathbf{F})$

35. Find the dual of each of these compound propositions.

- a)  $p \wedge \neg q \wedge \neg r$
- b)  $(p \wedge q \wedge r) \vee s$
- c)  $(p \vee \mathbf{F}) \wedge (q \vee \mathbf{T})$

36. When does  $s^* = s$ , where  $s$  is a compound proposition?


37. Show that  $(s^*)^* = s$  when  $s$  is a compound proposition.

38. Show that the logical equivalences in Table 6, except for the double negation law, come in pairs, where each pair contains compound propositions that are duals of each other.

**\*\*39.** Why are the duals of two equivalent compound propositions also equivalent, where these compound propositions contain only the operators  $\wedge$ ,  $\vee$ , and  $\neg$ ?

40. Find a compound proposition involving the propositional variables  $p$ ,  $q$ , and  $r$  that is true when  $p$  and  $q$  are true and  $r$  is false, but is false otherwise. [Hint: Use a conjunction of each propositional variable or its negation.]

41. Find a compound proposition involving the propositional variables  $p$ ,  $q$ , and  $r$  that is true when exactly two of  $p$ ,  $q$ , and  $r$  are true and is false otherwise. [Hint: Form a disjunction of conjunctions. Include a conjunction for each combination of values for which the compound proposition is true. Each conjunction should include each of the three propositional variables or its negations.]

 42. Suppose that a truth table in  $n$  propositional variables is specified. Show that a compound proposition with this truth table can be formed by taking the disjunction of conjunctions of the variables or their negations, with one conjunction included for each combination of values for which the compound proposition is true. The resulting compound proposition is said to be in **disjunctive normal form**.

A collection of logical operators is called **functionally complete** if every compound proposition is logically equivalent to a compound proposition involving only these logical operators.

43. Show that  $\neg$ ,  $\wedge$ , and  $\vee$  form a functionally complete collection of logical operators. [Hint: Use the fact that every compound proposition is logically equivalent to one in disjunctive normal form, as shown in Exercise 42.]

- \*44. Show that  $\neg$  and  $\wedge$  form a functionally complete collection of logical operators. [Hint: First use a De Morgan law to show that  $p \vee q$  is logically equivalent to  $\neg(\neg p \wedge \neg q)$ .]
- \*45. Show that  $\neg$  and  $\vee$  form a functionally complete collection of logical operators.
- The following exercises involve the logical operators *NAND* and *NOR*. The proposition  $p$  *NAND*  $q$  is true when either  $p$  or  $q$ , or both, are false; and it is false when both  $p$  and  $q$  are true. The proposition  $p$  *NOR*  $q$  is true when both  $p$  and  $q$  are false, and it is false otherwise. The propositions  $p$  *NAND*  $q$  and  $p$  *NOR*  $q$  are denoted by  $p \downarrow q$  and  $p \uparrow q$ , respectively. (The operators  $\downarrow$  and  $\uparrow$  are called the **Sheffer stroke** and the **Peirce arrow** after H. M. Sheffer and C. S. Peirce, respectively.)
46. Construct a truth table for the logical operator *NAND*.
47. Show that  $p \downarrow q$  is logically equivalent to  $\neg(p \wedge q)$ .
48. Construct a truth table for the logical operator *NOR*.
49. Show that  $p \downarrow q$  is logically equivalent to  $\neg(p \vee q)$ .
50. In this exercise we will show that  $\{\downarrow\}$  is a functionally complete collection of logical operators.
- Show that  $p \downarrow p$  is logically equivalent to  $\neg p$ .
  - Show that  $(p \downarrow q) \downarrow (p \downarrow q)$  is logically equivalent to  $p \vee q$ .
  - Conclude from parts (a) and (b), and Exercise 49, that  $\{\downarrow\}$  is a functionally complete collection of logical operators.
- \*51. Find a compound proposition logically equivalent to  $p \rightarrow q$  using only the logical operator  $\downarrow$ .
52. Show that  $\{\uparrow\}$  is a functionally complete collection of logical operators.
53. Show that  $p \downarrow q$  and  $q \downarrow p$  are equivalent.
54. Show that  $p \downarrow (q \downarrow r)$  and  $(p \downarrow q) \downarrow r$  are not equivalent, so that the logical operator  $\downarrow$  is not associative.
- \*55. How many different truth tables of compound propositions are there that involve the propositional variables  $p$  and  $q$ ?
56. Show that if  $p$ ,  $q$ , and  $r$  are compound propositions such that  $p$  and  $q$  are logically equivalent and  $q$  and  $r$  are logically equivalent, then  $p$  and  $r$  are logically equivalent.
57. The following sentence is taken from the specification of a telephone system: "If the directory database is opened, then the monitor is put in a closed state, if the system is not in its initial state." This specification is hard to under-

stand because it involves two conditional statements. Find an equivalent, easier-to-understand specification that involves disjunctions and negations but not conditional statements.

58. How many of the disjunctions  $p \vee \neg q$ ,  $\neg p \vee q$ ,  $q \vee r$ ,  $q \vee \neg r$ , and  $\neg q \vee \neg r$  can be made simultaneously true by an assignment of truth values to  $p$ ,  $q$ , and  $r$ ?
59. How many of the disjunctions  $p \vee \neg q \vee s$ ,  $\neg p \vee \neg r \vee s$ ,  $\neg p \vee \neg r \vee \neg s$ ,  $\neg p \vee q \vee \neg s$ ,  $q \vee r \vee \neg s$ ,  $q \vee \neg r \vee \neg s$ ,  $\neg p \vee \neg q \vee \neg s$ ,  $p \vee r \vee s$ , and  $p \vee r \vee \neg s$  can be made simultaneously true by an assignment of truth values to  $p$ ,  $q$ ,  $r$ , and  $s$ ?
60. Show that the negation of an unsatisfiable compound proposition is a tautology and the negation of a compound proposition that is a tautology is unsatisfiable.
61. Determine whether each of these compound propositions is satisfiable.
- $(p \vee \neg q) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg q)$
  - $(p \rightarrow q) \wedge (p \rightarrow \neg q) \wedge (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$
  - $(p \leftrightarrow q) \wedge (\neg p \leftrightarrow q)$
62. Determine whether each of these compound propositions is satisfiable.
- $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$
  - $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$
  - $(p \vee q \vee r) \wedge (p \vee \neg q \vee \neg s) \wedge (q \vee \neg r \vee s) \wedge (\neg p \vee r \vee s) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee s) \wedge (\neg p \vee \neg r \vee \neg s)$
63. Show how the solution of a given  $4 \times 4$  Sudoku puzzle can be found by solving a satisfiability problem.
64. Construct a compound proposition that asserts that every cell of a  $9 \times 9$  Sudoku puzzle contains at least one number.
65. Explain the steps in the construction of the compound proposition given in the text that asserts that every column of a  $9 \times 9$  Sudoku puzzle contains every number.
- \*66. Explain the steps in the construction of the compound proposition given in the text that asserts that each of the nine  $3 \times 3$  blocks of a  $9 \times 9$  Sudoku puzzle contains every number.

## 1.4 Predicates and Quantifiers

### Introduction

Propositional logic, studied in Sections 1.1–1.3, cannot adequately express the meaning of all statements in mathematics and in natural language. For example, suppose that we know that

“Every computer connected to the university network is functioning properly.”

## Exercises

- Let  $P(x)$  denote the statement " $x \leq 4$ ." What are these truth values?  
 a)  $P(0)$                       b)  $P(4)$                       c)  $P(6)$
- Let  $P(x)$  be the statement "the word  $x$  contains the letter  $a$ ." What are these truth values?  
 a)  $P(\text{orange})$               b)  $P(\text{lemon})$   
 c)  $P(\text{true})$                   d)  $P(\text{false})$
- Let  $Q(x, y)$  denote the statement " $x$  is the capital of  $y$ ." What are these truth values?  
 a)  $Q(\text{Denver, Colorado})$   
 b)  $Q(\text{Detroit, Michigan})$   
 c)  $Q(\text{Massachusetts, Boston})$   
 d)  $Q(\text{New York, New York})$
- State the value of  $x$  after the statement **if**  $P(x)$  **then**  $x := 1$  is executed, where  $P(x)$  is the statement " $x > 1$ ," if the value of  $x$  when this statement is reached is  
 a)  $x = 0$ .                              b)  $x = 1$ .  
 c)  $x = 2$ .
- Let  $P(x)$  be the statement " $x$  spends more than five hours every weekday in class," where the domain for  $x$  consists of all students. Express each of these quantifications in English.  
 a)  $\exists x P(x)$                       b)  $\forall x P(x)$   
 c)  $\exists x \neg P(x)$                   d)  $\forall x \neg P(x)$
- Let  $N(x)$  be the statement " $x$  has visited North Dakota," where the domain consists of the students in your school. Express each of these quantifications in English.  
 a)  $\exists x N(x)$                       b)  $\forall x N(x)$                       c)  $\neg \exists x N(x)$   
 d)  $\exists x \neg N(x)$                   e)  $\neg \forall x N(x)$                   f)  $\forall x \neg N(x)$
- Translate these statements into English, where  $C(x)$  is " $x$  is a comedian" and  $F(x)$  is " $x$  is funny" and the domain consists of all people.  
 a)  $\forall x (C(x) \rightarrow F(x))$               b)  $\forall x (C(x) \wedge F(x))$   
 c)  $\exists x (C(x) \rightarrow F(x))$               d)  $\exists x (C(x) \wedge F(x))$
- Translate these statements into English, where  $R(x)$  is " $x$  is a rabbit" and  $H(x)$  is " $x$  hops" and the domain consists of all animals.  
 a)  $\forall x (R(x) \rightarrow H(x))$               b)  $\forall x (R(x) \wedge H(x))$   
 c)  $\exists x (R(x) \rightarrow H(x))$               d)  $\exists x (R(x) \wedge H(x))$
- Let  $P(x)$  be the statement " $x$  can speak Russian" and let  $Q(x)$  be the statement " $x$  knows the computer language C++." Express each of these sentences in terms of  $P(x)$ ,  $Q(x)$ , quantifiers, and logical connectives. The domain for quantifiers consists of all students at your school.  
 a) There is a student at your school who can speak Russian and who knows C++.  
 b) There is a student at your school who can speak Russian but who doesn't know C++.  
 c) Every student at your school either can speak Russian or knows C++.  
 d) No student at your school can speak Russian or knows C++.
- Let  $C(x)$  be the statement " $x$  has a cat," let  $D(x)$  be the statement " $x$  has a dog," and let  $F(x)$  be the statement " $x$  has a ferret." Express each of these statements in terms of  $C(x)$ ,  $D(x)$ ,  $F(x)$ , quantifiers, and logical connectives. Let the domain consist of all students in your class.  
 a) A student in your class has a cat, a dog, and a ferret.  
 b) All students in your class have a cat, a dog, or a ferret.  
 c) Some student in your class has a cat and a ferret, but not a dog.  
 d) No student in your class has a cat, a dog, and a ferret.  
 e) For each of the three animals, cats, dogs, and ferrets, there is a student in your class who has this animal as a pet.
- Let  $P(x)$  be the statement " $x = x^2$ ." If the domain consists of the integers, what are these truth values?  
 a)  $P(0)$                               b)  $P(1)$                               c)  $P(2)$   
 d)  $P(-1)$                               e)  $\exists x P(x)$                               f)  $\forall x P(x)$
- Let  $Q(x)$  be the statement " $x + 1 > 2x$ ." If the domain consists of all integers, what are these truth values?  
 a)  $Q(0)$                               b)  $Q(-1)$                               c)  $Q(1)$   
 d)  $\exists x Q(x)$                               e)  $\forall x Q(x)$                               f)  $\exists x \neg Q(x)$   
 g)  $\forall x \neg Q(x)$
- Determine the truth value of each of these statements if the domain consists of all integers.  
 a)  $\forall n (n + 1 > n)$                       b)  $\exists n (2n = 3n)$   
 c)  $\exists n (n = -n)$                       d)  $\forall n (3n \leq 4n)$
- Determine the truth value of each of these statements if the domain consists of all real numbers.  
 a)  $\exists x (x^3 = -1)$                       b)  $\exists x (x^4 < x^2)$   
 c)  $\forall x ((-x)^2 = x^2)$                       d)  $\forall x (2x > x)$
- Determine the truth value of each of these statements if the domain for all variables consists of all integers.  
 a)  $\forall n (n^2 \geq 0)$                       b)  $\exists n (n^2 = 2)$   
 c)  $\forall n (n^2 \geq n)$                       d)  $\exists n (n^2 < 0)$
- Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.  
 a)  $\exists x (x^2 = 2)$                               b)  $\exists x (x^2 = -1)$   
 c)  $\forall x (x^2 + 2 \geq 1)$                       d)  $\forall x (x^2 \neq x)$
- Suppose that the domain of the propositional function  $P(x)$  consists of the integers 0, 1, 2, 3, and 4. Write out each of these propositions using disjunctions, conjunctions, and negations.  
 a)  $\exists x P(x)$                               b)  $\forall x P(x)$                               c)  $\exists x \neg P(x)$   
 d)  $\forall x \neg P(x)$                               e)  $\neg \exists x P(x)$                               f)  $\neg \forall x P(x)$
- Suppose that the domain of the propositional function  $P(x)$  consists of the integers  $-2, -1, 0, 1$ , and  $2$ . Write out each of these propositions using disjunctions, conjunctions, and negations.  
 a)  $\exists x P(x)$                               b)  $\forall x P(x)$                               c)  $\exists x \neg P(x)$   
 d)  $\forall x \neg P(x)$                               e)  $\neg \exists x P(x)$                               f)  $\neg \forall x P(x)$

19. Suppose that the domain of the propositional function  $P(x)$  consists of the integers 1, 2, 3, 4, and 5. Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.
- $\exists x P(x)$
  - $\forall x P(x)$
  - $\neg \exists x P(x)$
  - $\neg \forall x P(x)$
  - $\forall x ((x \neq 3) \rightarrow P(x)) \vee \exists x \neg P(x)$
20. Suppose that the domain of the propositional function  $P(x)$  consists of  $-5, -3, -1, 1, 3$ , and  $5$ . Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.
- $\exists x P(x)$
  - $\forall x P(x)$
  - $\forall x ((x \neq 1) \rightarrow P(x))$
  - $\exists x ((x \geq 0) \wedge P(x))$
  - $\exists x (\neg P(x)) \wedge \forall x ((x < 0) \rightarrow P(x))$
21. For each of these statements find a domain for which the statement is true and a domain for which the statement is false.
- Everyone is studying discrete mathematics.
  - Everyone is older than 21 years.
  - Every two people have the same mother.
  - No two different people have the same grandmother.
22. For each of these statements find a domain for which the statement is true and a domain for which the statement is false.
- Everyone speaks Hindi.
  - There is someone older than 21 years.
  - Every two people have the same first name.
  - Someone knows more than two other people.
23. Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people.
- Someone in your class can speak Hindi.
  - Everyone in your class is friendly.
  - There is a person in your class who was not born in California.
  - A student in your class has been in a movie.
  - No student in your class has taken a course in logic programming.
24. Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people.
- Everyone in your class has a cellular phone.
  - Somebody in your class has seen a foreign movie.
  - There is a person in your class who cannot swim.
  - All students in your class can solve quadratic equations.
  - Some student in your class does not want to be rich.
25. Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.
- No one is perfect.
  - Not everyone is perfect.
  - All your friends are perfect.
  - At least one of your friends is perfect.
  - Everyone is your friend and is perfect.
  - Not everybody is your friend or someone is not perfect.
26. Translate each of these statements into logical expressions in three different ways by varying the domain and by using predicates with one and with two variables.
- Someone in your school has visited Uzbekistan.
  - Everyone in your class has studied calculus and C++.
  - No one in your school owns both a bicycle and a motorcycle.
  - There is a person in your school who is not happy.
  - Everyone in your school was born in the twentieth century.
27. Translate each of these statements into logical expressions in three different ways by varying the domain and by using predicates with one and with two variables.
- A student in your school has lived in Vietnam.
  - There is a student in your school who cannot speak Hindi.
  - A student in your school knows Java, Prolog, and C++.
  - Everyone in your class enjoys Thai food.
  - Someone in your class does not play hockey.
28. Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.
- Something is not in the correct place.
  - All tools are in the correct place and are in excellent condition.
  - Everything is in the correct place and in excellent condition.
  - Nothing is in the correct place and is in excellent condition.
  - One of your tools is not in the correct place, but it is in excellent condition.
29. Express each of these statements using logical operators, predicates, and quantifiers.
- Some propositions are tautologies.
  - The negation of a contradiction is a tautology.
  - The disjunction of two contingencies can be a tautology.
  - The conjunction of two tautologies is a tautology.
30. Suppose the domain of the propositional function  $P(x, y)$  consists of pairs  $x$  and  $y$ , where  $x$  is 1, 2, or 3 and  $y$  is 1, 2, or 3. Write out these propositions using disjunctions and conjunctions.
- $\exists x P(x, 3)$
  - $\forall y P(1, y)$
  - $\exists y \neg P(2, y)$
  - $\forall x \neg P(x, 2)$
31. Suppose that the domain of  $Q(x, y, z)$  consists of triples  $x, y, z$ , where  $x = 0, 1$ , or  $2$ ,  $y = 0$  or  $1$ , and  $z = 0$  or  $1$ . Write out these propositions using disjunctions and conjunctions.
- $\forall y Q(0, y, 0)$
  - $\exists x Q(x, 1, 1)$
  - $\exists z \neg Q(0, 0, z)$
  - $\exists x \neg Q(x, 0, 1)$

- 32.** Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase “It is not the case that.”)
- All dogs have fleas.
  - There is a horse that can add.
  - Every koala can climb.
  - No monkey can speak French.
  - There exists a pig that can swim and catch fish.
- 33.** Express each of these statements using quantifiers. Then form the negation of the statement, so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase “It is not the case that.”)
- Some old dogs can learn new tricks.
  - No rabbit knows calculus.
  - Every bird can fly.
  - There is no dog that can talk.
  - There is no one in this class who knows French and Russian.
- 34.** Express the negation of these propositions using quantifiers, and then express the negation in English.
- Some drivers do not obey the speed limit.
  - All Swedish movies are serious.
  - No one can keep a secret.
  - There is someone in this class who does not have a good attitude.
- 35.** Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.
- $\forall x(x^2 \geq x)$
  - $\forall x(x > 0 \vee x < 0)$
  - $\forall x(x = 1)$
- 36.** Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all real numbers.
- $\forall x(x^2 \neq x)$
  - $\forall x(x^2 \neq 2)$
  - $\forall x(|x| > 0)$
- 37.** Express each of these statements using predicates and quantifiers.
- A passenger on an airline qualifies as an elite flyer if the passenger flies more than 25,000 miles in a year or takes more than 25 flights during that year.
  - A man qualifies for the marathon if his best previous time is less than 3 hours and a woman qualifies for the marathon if her best previous time is less than 3.5 hours.
  - A student must take at least 60 course hours, or at least 45 course hours and write a master’s thesis, and receive a grade no lower than a B in all required courses, to receive a master’s degree.
  - There is a student who has taken more than 21 credit hours in a semester and received all A’s.
- Exercises 38–42 deal with the translation between system specification and logical expressions involving quantifiers.
- 38.** Translate these system specifications into English where the predicate  $S(x, y)$  is “ $x$  is in state  $y$ ” and where the domain for  $x$  and  $y$  consists of all systems and all possible states, respectively.
- $\exists x S(x, \text{open})$
  - $\forall x (S(x, \text{malfunctioning}) \vee S(x, \text{diagnostic}))$
  - $\exists x S(x, \text{open}) \vee \exists x S(x, \text{diagnostic})$
  - $\exists x \neg S(x, \text{available})$
  - $\forall x \neg S(x, \text{working})$
- 39.** Translate these specifications into English where  $F(p)$  is “Printer  $p$  is out of service,”  $B(p)$  is “Printer  $p$  is busy,”  $L(j)$  is “Print job  $j$  is lost,” and  $Q(j)$  is “Print job  $j$  is queued.”
- $\exists p (F(p) \wedge B(p)) \rightarrow \exists j L(j)$
  - $\forall p B(p) \rightarrow \exists j Q(j)$
  - $\exists j (Q(j) \wedge L(j)) \rightarrow \exists p F(p)$
  - $(\forall p B(p) \wedge \forall j Q(j)) \rightarrow \exists j L(j)$
- 40.** Express each of these system specifications using predicates, quantifiers, and logical connectives.
- When there is less than 30 megabytes free on the hard disk, a warning message is sent to all users.
  - No directories in the file system can be opened and no files can be closed when system errors have been detected.
  - The file system cannot be backed up if there is a user currently logged on.
  - Video on demand can be delivered when there are at least 8 megabytes of memory available and the connection speed is at least 56 kilobits per second.
- 41.** Express each of these system specifications using predicates, quantifiers, and logical connectives.
- At least one mail message, among the nonempty set of messages, can be saved if there is a disk with more than 10 kilobytes of free space.
  - Whenever there is an active alert, all queued messages are transmitted.
  - The diagnostic monitor tracks the status of all systems except the main console.
  - Each participant on the conference call whom the host of the call did not put on a special list was billed.
- 42.** Express each of these system specifications using predicates, quantifiers, and logical connectives.
- Every user has access to an electronic mailbox.
  - The system mailbox can be accessed by everyone in the group if the file system is locked.
  - The firewall is in a diagnostic state only if the proxy server is in a diagnostic state.
  - At least one router is functioning normally if the throughput is between 100 kbps and 500 kbps and the proxy server is not in diagnostic mode.



43. Determine whether  $\forall x(P(x) \rightarrow Q(x))$  and  $\forall x P(x) \rightarrow \forall x Q(x)$  are logically equivalent. Justify your answer.
44. Determine whether  $\forall x(P(x) \leftrightarrow Q(x))$  and  $\forall x P(x) \leftrightarrow \forall x Q(x)$  are logically equivalent. Justify your answer.
45. Show that  $\exists x(P(x) \vee Q(x))$  and  $\exists x P(x) \vee \exists x Q(x)$  are logically equivalent.

Exercises 46–49 establish rules for **null quantification** that we can use when a quantified variable does not appear in part of a statement.

46. Establish these logical equivalences, where  $x$  does not occur as a free variable in  $A$ . Assume that the domain is nonempty.
- $(\forall x P(x)) \vee A \equiv \forall x(P(x) \vee A)$
  - $(\exists x P(x)) \vee A \equiv \exists x(P(x) \vee A)$
47. Establish these logical equivalences, where  $x$  does not occur as a free variable in  $A$ . Assume that the domain is nonempty.
- $(\forall x P(x)) \wedge A \equiv \forall x(P(x) \wedge A)$
  - $(\exists x P(x)) \wedge A \equiv \exists x(P(x) \wedge A)$
48. Establish these logical equivalences, where  $x$  does not occur as a free variable in  $A$ . Assume that the domain is nonempty.
- $\forall x(A \rightarrow P(x)) \equiv A \rightarrow \forall x P(x)$
  - $\exists x(A \rightarrow P(x)) \equiv A \rightarrow \exists x P(x)$
49. Establish these logical equivalences, where  $x$  does not occur as a free variable in  $A$ . Assume that the domain is nonempty.
- $\forall x(P(x) \rightarrow A) \equiv \exists x P(x) \rightarrow A$
  - $\exists x(P(x) \rightarrow A) \equiv \forall x P(x) \rightarrow A$
50. Show that  $\forall x P(x) \vee \forall x Q(x)$  and  $\forall x(P(x) \vee Q(x))$  are not logically equivalent.
51. Show that  $\exists x P(x) \wedge \exists x Q(x)$  and  $\exists x(P(x) \wedge Q(x))$  are not logically equivalent.
52. As mentioned in the text, the notation  $\exists! x P(x)$  denotes “There exists a unique  $x$  such that  $P(x)$  is true.”

If the domain consists of all integers, what are the truth values of these statements?

- $\exists! x(x > 1)$
  - $\exists! x(x^2 = 1)$
  - $\exists! x(x + 3 = 2x)$
  - $\exists! x(x = x + 1)$
53. What are the truth values of these statements?
- $\exists! x P(x) \rightarrow \exists x P(x)$
  - $\forall x P(x) \rightarrow \exists! x P(x)$
  - $\exists! x \neg P(x) \rightarrow \neg \forall x P(x)$
54. Write out  $\exists! x P(x)$ , where the domain consists of the integers 1, 2, and 3, in terms of negations, conjunctions, and disjunctions.
55. Given the Prolog facts in Example 28, what would Prolog return given these queries?
- `?instructor(chan, math273)`
  - `?instructor(patel, cs301)`
  - `?enrolled(X, cs301)`
  - `?enrolled(kiko, Y)`
  - `?teaches(grossman, Y)`

56. Given the Prolog facts in Example 28, what would Prolog return when given these queries?
- `?enrolled(kevin, ee222)`
  - `?enrolled(kiko, math273)`
  - `?instructor(grossman, X)`
  - `?instructor(X, cs301)`
  - `?teaches(X, kevin)`
57. Suppose that Prolog facts are used to define the predicates *mother*( $M, Y$ ) and *father*( $F, X$ ), which represent that  $M$  is the mother of  $Y$  and  $F$  is the father of  $X$ , respectively. Give a Prolog rule to define the predicate *sibling*( $X, Y$ ), which represents that  $X$  and  $Y$  are siblings (that is, have the same mother and the same father).

58. Suppose that Prolog facts are used to define the predicates *mother*( $M, Y$ ) and *father*( $F, X$ ), which represent that  $M$  is the mother of  $Y$  and  $F$  is the father of  $X$ , respectively. Give a Prolog rule to define the predicate *grandfather*( $X, Y$ ), which represents that  $X$  is the grandfather of  $Y$ . [Hint: You can write a disjunction in Prolog either by using a semicolon to separate predicates or by putting these predicates on separate lines.]

Exercises 59–62 are based on questions found in the book *Symbolic Logic* by Lewis Carroll.

59. Let  $P(x)$ ,  $Q(x)$ , and  $R(x)$  be the statements “ $x$  is a professor,” “ $x$  is ignorant,” and “ $x$  is vain,” respectively. Express each of these statements using quantifiers; logical connectives; and  $P(x)$ ,  $Q(x)$ , and  $R(x)$ , where the domain consists of all people.
- No professors are ignorant.
  - All ignorant people are vain.
  - No professors are vain.
  - Does (c) follow from (a) and (b)?
60. Let  $P(x)$ ,  $Q(x)$ , and  $R(x)$  be the statements “ $x$  is a clear explanation,” “ $x$  is satisfactory,” and “ $x$  is an excuse,” respectively. Suppose that the domain for  $x$  consists of all English text. Express each of these statements using quantifiers, logical connectives, and  $P(x)$ ,  $Q(x)$ , and  $R(x)$ .
- All clear explanations are satisfactory.
  - Some excuses are unsatisfactory.
  - Some excuses are not clear explanations.
  - \*d) Does (c) follow from (a) and (b)?
61. Let  $P(x)$ ,  $Q(x)$ ,  $R(x)$ , and  $S(x)$  be the statements “ $x$  is a baby,” “ $x$  is logical,” “ $x$  is able to manage a crocodile,” and “ $x$  is despised,” respectively. Suppose that the domain consists of all people. Express each of these statements using quantifiers; logical connectives; and  $P(x)$ ,  $Q(x)$ ,  $R(x)$ , and  $S(x)$ .
- Babies are illogical.
  - Nobody is despised who can manage a crocodile.
  - Illogical persons are despised.
  - Babies cannot manage crocodiles.
  - \*e) Does (d) follow from (a), (b), and (c)? If not, is there a correct conclusion?

**EXAMPLE 16** (*Requires calculus*) Use quantifiers and predicates to express the fact that  $\lim_{x \rightarrow a} f(x)$  does not exist where  $f(x)$  is a real-valued function of a real variable  $x$  and  $a$  belongs to the domain of  $f$ .

**Solution:** To say that  $\lim_{x \rightarrow a} f(x)$  does not exist means that for all real numbers  $L$ ,  $\lim_{x \rightarrow a} f(x) \neq L$ . By using Example 8, the statement  $\lim_{x \rightarrow a} f(x) \neq L$  can be expressed as

$$\neg \forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon).$$


Successively applying the rules for negating quantified expressions, we construct this sequence of equivalent statements

$$\begin{aligned} & \neg \forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\ & \equiv \exists \epsilon > 0 \neg \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\ & \equiv \exists \epsilon > 0 \forall \delta > 0 \neg \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\ & \equiv \exists \epsilon > 0 \forall \delta > 0 \exists x \neg (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\ & \equiv \exists \epsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon). \end{aligned}$$

In the last step we used the equivalence  $\neg(p \rightarrow q) \equiv p \wedge \neg q$ , which follows from the fifth equivalence in Table 7 of Section 1.3.

Because the statement “ $\lim_{x \rightarrow a} f(x)$  does not exist” means for all real numbers  $L$ ,  $\lim_{x \rightarrow a} f(x) \neq L$ , this can be expressed as

$$\forall L \exists \epsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon).$$

This last statement says that for every real number  $L$  there is a real number  $\epsilon > 0$  such that for every real number  $\delta > 0$ , there exists a real number  $x$  such that  $0 < |x - a| < \delta$  and  $|f(x) - L| \geq \epsilon$ . 

## Exercises

- Translate these statements into English, where the domain for each variable consists of all real numbers.
  - $\forall x \exists y (x < y)$
  - $\forall x \forall y (((x \geq 0) \wedge (y \geq 0)) \rightarrow (xy \geq 0))$
  - $\forall x \forall y \exists z (xy = z)$
- Translate these statements into English, where the domain for each variable consists of all real numbers.
  - $\exists x \forall y (xy = y)$
  - $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$
  - $\forall x \forall y \exists z (x = y + z)$
- Let  $Q(x, y)$  be the statement “ $x$  has sent an e-mail message to  $y$ ,” where the domain for both  $x$  and  $y$  consists of all students in your class. Express each of these quantifications in English.
  - $\exists x \exists y Q(x, y)$
  - $\exists x \forall y Q(x, y)$
  - $\forall x \exists y Q(x, y)$
  - $\exists y \forall x Q(x, y)$
  - $\forall y \exists x Q(x, y)$
  - $\forall x \forall y Q(x, y)$
- Let  $P(x, y)$  be the statement “Student  $x$  has taken class  $y$ ,” where the domain for  $x$  consists of all students in your class and for  $y$  consists of all computer science courses at your school. Express each of these quantifications in English.
  - $\exists x \exists y P(x, y)$
  - $\exists x \forall y P(x, y)$
  - $\forall x \exists y P(x, y)$
  - $\exists y \forall x P(x, y)$
  - $\forall y \exists x P(x, y)$
  - $\forall x \forall y P(x, y)$
- Let  $W(x, y)$  mean that student  $x$  has visited website  $y$ , where the domain for  $x$  consists of all students in your school and the domain for  $y$  consists of all websites. Express each of these statements by a simple English sentence.
  - $W(\text{Sarah Smith}, \text{www.att.com})$
  - $\exists x W(x, \text{www.imdb.org})$
  - $\exists y W(\text{José Orez}, y)$
  - $\exists y (W(\text{Ashok Puri}, y) \wedge W(\text{Cindy Yoon}, y))$
  - $\exists y \forall z (y \neq (\text{David Belcher}) \wedge (W(\text{David Belcher}, z) \rightarrow W(y, z)))$
  - $\exists x \exists y \forall z ((x \neq y) \wedge (W(x, z) \leftrightarrow W(y, z)))$
- Let  $C(x, y)$  mean that student  $x$  is enrolled in class  $y$ , where the domain for  $x$  consists of all students in your school and the domain for  $y$  consists of all classes being



given at your school. Express each of these statements by a simple English sentence.

- a)  $C(\text{Randy Goldberg, CS 252})$
  - b)  $\exists x C(x, \text{Math 695})$
  - c)  $\exists y C(\text{Carol Sitea, } y)$
  - d)  $\exists x (C(x, \text{Math 222}) \wedge C(x, \text{CS 252}))$
  - e)  $\exists x \exists y \forall z ((x \neq y) \wedge (C(x, z) \rightarrow C(y, z)))$
  - f)  $\exists x \exists y \forall z ((x \neq y) \wedge (C(x, z) \leftrightarrow C(y, z)))$
7. Let  $T(x, y)$  mean that student  $x$  likes cuisine  $y$ , where the domain for  $x$  consists of all students at your school and the domain for  $y$  consists of all cuisines. Express each of these statements by a simple English sentence.
- a)  $\neg T(\text{Abdallah Hussein, Japanese})$
  - b)  $\exists x T(x, \text{Korean}) \wedge \forall x T(x, \text{Mexican})$
  - c)  $\exists y (T(\text{Monique Arsenault, } y) \vee T(\text{Jay Johnson, } y))$
  - d)  $\forall x \forall z \exists y ((x \neq z) \rightarrow \neg (T(x, y) \wedge T(z, y)))$
  - e)  $\exists x \exists z \forall y (T(x, y) \leftrightarrow T(z, y))$
  - f)  $\forall x \forall z \exists y (T(x, y) \leftrightarrow T(z, y))$
8. Let  $Q(x, y)$  be the statement “student  $x$  has been a contestant on quiz show  $y$ .” Express each of these sentences in terms of  $Q(x, y)$ , quantifiers, and logical connectives, where the domain for  $x$  consists of all students at your school and for  $y$  consists of all quiz shows on television.
- a) There is a student at your school who has been a contestant on a television quiz show.
  - b) No student at your school has ever been a contestant on a television quiz show.
  - c) There is a student at your school who has been a contestant on *Jeopardy* and on *Wheel of Fortune*.
  - d) Every television quiz show has had a student from your school as a contestant.
  - e) At least two students from your school have been contestants on *Jeopardy*.
9. Let  $L(x, y)$  be the statement “ $x$  loves  $y$ ,” where the domain for both  $x$  and  $y$  consists of all people in the world. Use quantifiers to express each of these statements.
- a) Everybody loves Jerry.
  - b) Everybody loves somebody.
  - c) There is somebody whom everybody loves.
  - d) Nobody loves everybody.
  - e) There is somebody whom Lydia does not love.
  - f) There is somebody whom no one loves.
  - g) There is exactly one person whom everybody loves.
  - h) There are exactly two people whom Lynn loves.
  - i) Everyone loves himself or herself.
  - j) There is someone who loves no one besides himself or herself.
10. Let  $F(x, y)$  be the statement “ $x$  can fool  $y$ ,” where the domain consists of all people in the world. Use quantifiers to express each of these statements.
- a) Everybody can fool Fred.
  - b) Evelyn can fool everybody.
  - c) Everybody can fool somebody.
  - d) There is no one who can fool everybody.
  - e) Everyone can be fooled by somebody.
  - f) No one can fool both Fred and Jerry.
  - g) Nancy can fool exactly two people.
  - h) There is exactly one person whom everybody can fool.
  - i) No one can fool himself or herself.
  - j) There is someone who can fool exactly one person besides himself or herself.
11. Let  $S(x)$  be the predicate “ $x$  is a student,”  $F(x)$  the predicate “ $x$  is a faculty member,” and  $A(x, y)$  the predicate “ $x$  has asked  $y$  a question,” where the domain consists of all people associated with your school. Use quantifiers to express each of these statements.
- a) Lois has asked Professor Michaels a question.
  - b) Every student has asked Professor Gross a question.
  - c) Every faculty member has either asked Professor Miller a question or been asked a question by Professor Miller.
  - d) Some student has not asked any faculty member a question.
  - e) There is a faculty member who has never been asked a question by a student.
  - f) Some student has asked every faculty member a question.
  - g) There is a faculty member who has asked every other faculty member a question.
  - h) Some student has never been asked a question by a faculty member.
12. Let  $I(x)$  be the statement “ $x$  has an Internet connection” and  $C(x, y)$  be the statement “ $x$  and  $y$  have chatted over the Internet,” where the domain for the variables  $x$  and  $y$  consists of all students in your class. Use quantifiers to express each of these statements.
- a) Jerry does not have an Internet connection.
  - b) Rachel has not chatted over the Internet with Chelsea.
  - c) Jan and Sharon have never chatted over the Internet.
  - d) No one in the class has chatted with Bob.
  - e) Sanjay has chatted with everyone except Joseph.
  - f) Someone in your class does not have an Internet connection.
  - g) Not everyone in your class has an Internet connection.
  - h) Exactly one student in your class has an Internet connection.
  - i) Everyone except one student in your class has an Internet connection.
  - j) Everyone in your class with an Internet connection has chatted over the Internet with at least one other student in your class.
  - k) Someone in your class has an Internet connection but has not chatted with anyone else in your class.
  - l) There are two students in your class who have not chatted with each other over the Internet.
  - m) There is a student in your class who has chatted with everyone in your class over the Internet.
  - n) There are at least two students in your class who have not chatted with the same person in your class.
  - o) There are two students in the class who between them have chatted with everyone else in the class.

13. Let  $M(x, y)$  be “ $x$  has sent  $y$  an e-mail message” and  $T(x, y)$  be “ $x$  has telephoned  $y$ ,” where the domain consists of all students in your class. Use quantifiers to express each of these statements. (Assume that all e-mail messages that were sent are received, which is not the way things often work.)
- Chou has never sent an e-mail message to Koko.
  - Arlene has never sent an e-mail message to or telephoned Sarah.
  - José has never received an e-mail message from Deborah.
  - Every student in your class has sent an e-mail message to Ken.
  - No one in your class has telephoned Nina.
  - Everyone in your class has either telephoned Avi or sent him an e-mail message.
  - There is a student in your class who has sent everyone else in your class an e-mail message.
  - There is someone in your class who has either sent an e-mail message or telephoned everyone else in your class.
  - There are two different students in your class who have sent each other e-mail messages.
  - There is a student who has sent himself or herself an e-mail message.
  - There is a student in your class who has not received an e-mail message from anyone else in the class and who has not been called by any other student in the class.
  - Every student in the class has either received an e-mail message or received a telephone call from another student in the class.
  - There are at least two students in your class such that one student has sent the other e-mail and the second student has telephoned the first student.
  - There are two different students in your class who between them have sent an e-mail message to or telephoned everyone else in the class.
14. Use quantifiers and predicates with more than one variable to express these statements.
- There is a student in this class who can speak Hindi.
  - Every student in this class plays some sport.
  - Some student in this class has visited Alaska but has not visited Hawaii.
  - All students in this class have learned at least one programming language.
  - There is a student in this class who has taken every course offered by one of the departments in this school.
  - Some student in this class grew up in the same town as exactly one other student in this class.
  - Every student in this class has chatted with at least one other student in at least one chat group.
15. Use quantifiers and predicates with more than one variable to express these statements.
- Every computer science student needs a course in discrete mathematics.
  - There is a student in this class who owns a personal computer.
  - Every student in this class has taken at least one computer science course.
  - There is a student in this class who has taken at least one course in computer science.
  - Every student in this class has been in every building on campus.
  - There is a student in this class who has been in every room of at least one building on campus.
  - Every student in this class has been in at least one room of every building on campus.
16. A discrete mathematics class contains 1 mathematics major who is a freshman, 12 mathematics majors who are sophomores, 15 computer science majors who are sophomores, 2 mathematics majors who are juniors, 2 computer science majors who are juniors, and 1 computer science major who is a senior. Express each of these statements in terms of quantifiers and then determine its truth value.
- There is a student in the class who is a junior.
  - Every student in the class is a computer science major.
  - There is a student in the class who is neither a mathematics major nor a junior.
  - Every student in the class is either a sophomore or a computer science major.
  - There is a major such that there is a student in the class in every year of study with that major.
17. Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.
- Every user has access to exactly one mailbox.
  - There is a process that continues to run during all error conditions only if the kernel is working correctly.
  - All users on the campus network can access all web-sites whose url has a .edu extension.
- \*d) There are exactly two systems that monitor every remote server.
18. Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.
- At least one console must be accessible during every fault condition.
  - The e-mail address of every user can be retrieved whenever the archive contains at least one message sent by every user on the system.
  - For every security breach there is at least one mechanism that can detect that breach if and only if there is a process that has not been compromised.
  - There are at least two paths connecting every two distinct endpoints on the network.
  - No one knows the password of every user on the system except for the system administrator, who knows all passwords.
19. Express each of these statements using mathematical and logical operators, predicates, and quantifiers, where the domain consists of all integers.
- The sum of two negative integers is negative.
  - The difference of two positive integers is not necessarily positive.

- c) The sum of the squares of two integers is greater than or equal to the square of their sum.  
 d) The absolute value of the product of two integers is the product of their absolute values.
20. Express each of these statements using predicates, quantifiers, logical connectives, and mathematical operators where the domain consists of all integers.
- The product of two negative integers is positive.
  - The average of two positive integers is positive.
  - The difference of two negative integers is not necessarily negative.
  - The absolute value of the sum of two integers does not exceed the sum of the absolute values of these integers.
21. Use predicates, quantifiers, logical connectives, and mathematical operators to express the statement that every positive integer is the sum of the squares of four integers.
22. Use predicates, quantifiers, logical connectives, and mathematical operators to express the statement that there is a positive integer that is not the sum of three squares.
23. Express each of these mathematical statements using predicates, quantifiers, logical connectives, and mathematical operators.
- The product of two negative real numbers is positive.
  - The difference of a real number and itself is zero.
  - Every positive real number has exactly two square roots.
  - A negative real number does not have a square root that is a real number.
24. Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers.
- $\exists x \forall y (x + y = y)$
  - $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$
  - $\exists x \exists y (((x \leq 0) \wedge (y \leq 0)) \wedge (x - y > 0))$
  - $\forall x \forall y ((x \neq 0) \wedge (y \neq 0) \leftrightarrow (xy \neq 0))$
25. Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers.
- $\exists x \forall y (xy = y)$
  - $\forall x \forall y (((x < 0) \wedge (y < 0)) \rightarrow (xy > 0))$
  - $\exists x \exists y ((x^2 > y) \wedge (x < y))$
  - $\forall x \forall y \exists z (x + y = z)$
26. Let  $Q(x, y)$  be the statement “ $x + y = x - y$ .” If the domain for both variables consists of all integers, what are the truth values?
- $Q(1, 1)$
  - $Q(2, 0)$
  - $\forall y Q(1, y)$
  - $\exists x Q(x, 2)$
  - $\exists x \exists y Q(x, y)$
  - $\forall x \exists y Q(x, y)$
  - $\exists y \forall x Q(x, y)$
  - $\forall y \exists x Q(x, y)$
  - $\forall x \forall y Q(x, y)$
27. Determine the truth value of each of these statements if the domain for all variables consists of all integers.
- $\forall n \exists m (n^2 < m)$
  - $\exists n \forall m (n < m^2)$
  - $\forall n \exists m (n + m = 0)$
  - $\exists n \forall m (nm = m)$
- $\exists n \exists m (n^2 + m^2 = 5)$
  - $\exists n \exists m (n + m = 4 \wedge n - m = 1)$
  - $\exists n \exists m (n + m = 4 \wedge n - m = 2)$
  - $\forall n \forall m \exists p (p = (m + n)/2)$
28. Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.
- $\forall x \exists y (x^2 = y)$
  - $\forall x \exists y (x = y^2)$
  - $\exists x \forall y (xy = 0)$
  - $\exists x \exists y (x + y \neq y + x)$
  - $\forall x (x \neq 0 \rightarrow \exists y (xy = 1))$
  - $\exists x \forall y (y \neq 0 \rightarrow xy = 1)$
  - $\forall x \exists y (x + y = 1)$
  - $\exists x \exists y (x + 2y = 2 \wedge 2x + 4y = 5)$
  - $\forall x \exists y (x + y = 2 \wedge 2x - y = 1)$
  - $\forall x \forall y \exists z (z = (x + y)/2)$
29. Suppose the domain of the propositional function  $P(x, y)$  consists of pairs  $x$  and  $y$ , where  $x$  is 1, 2, or 3 and  $y$  is 1, 2, or 3. Write out these propositions using disjunctions and conjunctions.
- $\forall x \forall y P(x, y)$
  - $\exists x \exists y P(x, y)$
  - $\exists x \forall y P(x, y)$
  - $\forall y \exists x P(x, y)$
30. Rewrite each of these statements so that negations appear only within predicates (that is, so that no negation is outside a quantifier or an expression involving logical connectives).
- $\neg \exists y \exists x P(x, y)$
  - $\neg \forall x \exists y P(x, y)$
  - $\neg \exists y (Q(y) \wedge \forall x \neg R(x, y))$
  - $\neg \exists y (\exists x R(x, y) \vee \forall x S(x, y))$
  - $\neg \exists y (\forall x \exists z T(x, y, z) \vee \exists x \forall z U(x, y, z))$
31. Express the negations of each of these statements so that all negation symbols immediately precede predicates.
- $\forall x \exists y \forall z T(x, y, z)$
  - $\forall x \exists y P(x, y) \vee \forall x \exists y Q(x, y)$
  - $\forall x \exists y (P(x, y) \wedge \exists z R(x, y, z))$
  - $\forall x \exists y (P(x, y) \rightarrow Q(x, y))$
32. Express the negations of each of these statements so that all negation symbols immediately precede predicates.
- $\exists z \forall y \forall x T(x, y, z)$
  - $\exists x \exists y P(x, y) \wedge \forall x \forall y Q(x, y)$
  - $\exists x \exists y (Q(x, y) \leftrightarrow Q(y, x))$
  - $\forall y \exists x \exists z (T(x, y, z) \vee Q(x, y))$
33. Rewrite each of these statements so that negations appear only within predicates (that is, so that no negation is outside a quantifier or an expression involving logical connectives).
- $\neg \forall x \forall y P(x, y)$
  - $\neg \forall y \exists x P(x, y)$
  - $\neg \forall y \forall x (P(x, y) \vee Q(x, y))$
  - $\neg (\exists x \exists y \neg P(x, y) \wedge \forall x \forall y Q(x, y))$
  - $\neg \forall x (\exists y \forall z P(x, y, z) \wedge \exists z \forall y P(x, y, z))$
34. Find a common domain for the variables  $x$ ,  $y$ , and  $z$  for which the statement  $\forall x \forall y ((x \neq y) \rightarrow \forall z ((z = x) \vee (z = y)))$  is true and another domain for which it is false.
35. Find a common domain for the variables  $x$ ,  $y$ ,  $z$ , and  $w$  for which the statement  $\forall x \forall y \forall z \exists w ((w \neq x) \wedge (w \neq y) \wedge (w \neq z))$  is true and another common domain for these variables for which it is false.

36. Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase “It is not the case that.”)
- No one has lost more than one thousand dollars playing the lottery.
  - There is a student in this class who has chatted with exactly one other student.
  - No student in this class has sent e-mail to exactly two other students in this class.
  - Some student has solved every exercise in this book.
  - No student has solved at least one exercise in every section of this book.
37. Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase “It is not the case that.”)
- Every student in this class has taken exactly two mathematics classes at this school.
  - Someone has visited every country in the world except Libya.
  - No one has climbed every mountain in the Himalayas.
  - Every movie actor has either been in a movie with Kevin Bacon or has been in a movie with someone who has been in a movie with Kevin Bacon.
38. Express the negations of these propositions using quantifiers, and in English.
- Every student in this class likes mathematics.
  - There is a student in this class who has never seen a computer.
  - There is a student in this class who has taken every mathematics course offered at this school.
  - There is a student in this class who has been in at least one room of every building on campus.
39. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.
- $\forall x \forall y (x^2 = y^2 \rightarrow x = y)$
  - $\forall x \exists y (y^2 = x)$
  - $\forall x \forall y (xy \geq x)$
40. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.
- $\forall x \exists y (x = 1/y)$
  - $\forall x \exists y (y^2 - x < 100)$
  - $\forall x \forall y (x^2 \neq y^3)$
41. Use quantifiers to express the associative law for multiplication of real numbers.
42. Use quantifiers to express the distributive laws of multiplication over addition for real numbers.
43. Use quantifiers and logical connectives to express the fact that every linear polynomial (that is, polynomial of degree 1) with real coefficients and where the coefficient of  $x$  is nonzero, has exactly one real root.
44. Use quantifiers and logical connectives to express the fact that a quadratic polynomial with real number coefficients has at most two real roots.

45. Determine the truth value of the statement  $\forall x \exists y (xy = 1)$  if the domain for the variables consists of
- the nonzero real numbers.
  - the nonzero integers.
  - the positive real numbers.
46. Determine the truth value of the statement  $\exists x \forall y (x \leq y^2)$  if the domain for the variables consists of
- the positive real numbers.
  - the integers.
  - the nonzero real numbers.
47. Show that the two statements  $\neg \exists x \forall y P(x, y)$  and  $\forall x \exists y \neg P(x, y)$ , where both quantifiers over the first variable in  $P(x, y)$  have the same domain, and both quantifiers over the second variable in  $P(x, y)$  have the same domain, are logically equivalent.
- \*48. Show that  $\forall x P(x) \vee \forall x Q(x)$  and  $\forall x \forall y (P(x) \vee Q(y))$ , where all quantifiers have the same nonempty domain, are logically equivalent. (The new variable  $y$  is used to combine the quantifications correctly.)
- \*49. a) Show that  $\forall x P(x) \wedge \exists x Q(x)$  is logically equivalent to  $\forall x \exists y (P(x) \wedge Q(y))$ , where all quantifiers have the same nonempty domain.
- b) Show that  $\forall x P(x) \vee \exists x Q(x)$  is equivalent to  $\forall x \exists y (P(x) \vee Q(y))$ , where all quantifiers have the same nonempty domain.

A statement is in **prenex normal form (PNF)** if and only if it is of the form

$$Q_1 x_1 Q_2 x_2 \cdots Q_k x_k P(x_1, x_2, \dots, x_k),$$

where each  $Q_i, i = 1, 2, \dots, k$ , is either the existential quantifier or the universal quantifier, and  $P(x_1, \dots, x_k)$  is a predicate involving no quantifiers. For example,  $\exists x \forall y (P(x, y) \wedge Q(y))$  is in prenex normal form, whereas  $\exists x P(x) \vee \forall x Q(x)$  is not (because the quantifiers do not all occur first).

Every statement formed from propositional variables, predicates, **T**, and **F** using logical connectives and quantifiers is equivalent to a statement in prenex normal form. Exercise 51 asks for a proof of this fact.

- \*50. Put these statements in prenex normal form. [Hint: Use logical equivalence from Tables 6 and 7 in Section 1.3, Table 2 in Section 1.4, Example 19 in Section 1.4, Exercises 45 and 46 in Section 1.4, and Exercises 48 and 49.]
- $\exists x P(x) \vee \exists x Q(x) \vee A$ , where  $A$  is a proposition not involving any quantifiers.
  - $\neg(\forall x P(x) \vee \forall x Q(x))$
  - $\exists x P(x) \rightarrow \exists x Q(x)$
- \*\*51. Show how to transform an arbitrary statement to a statement in prenex normal form that is equivalent to the given statement. (Note: A formal solution of this exercise requires use of structural induction, covered in Section 5.3.)
- \*52. Express the quantification  $\exists! x P(x)$ , introduced in Section 1.4, using universal quantifications, existential quantifications, and logical operators.


## Truth Sets and Quantifiers

We will now tie together concepts from set theory and from predicate logic. Given a predicate  $P$ , and a domain  $D$ , we define the **truth set** of  $P$  to be the set of elements  $x$  in  $D$  for which  $P(x)$  is true. The truth set of  $P(x)$  is denoted by  $\{x \in D \mid P(x)\}$ .

**EXAMPLE 23** What are the truth sets of the predicates  $P(x)$ ,  $Q(x)$ , and  $R(x)$ , where the domain is the set of integers and  $P(x)$  is “ $|x| = 1$ ,”  $Q(x)$  is “ $x^2 = 2$ ,” and  $R(x)$  is “ $|x| = x$ .”

**Solution:** The truth set of  $P$ ,  $\{x \in \mathbf{Z} \mid |x| = 1\}$ , is the set of integers for which  $|x| = 1$ . Because  $|x| = 1$  when  $x = 1$  or  $x = -1$ , and for no other integers  $x$ , we see that the truth set of  $P$  is the set  $\{-1, 1\}$ .

The truth set of  $Q$ ,  $\{x \in \mathbf{Z} \mid x^2 = 2\}$ , is the set of integers for which  $x^2 = 2$ . This is the empty set because there are no integers  $x$  for which  $x^2 = 2$ .

The truth set of  $R$ ,  $\{x \in \mathbf{Z} \mid |x| = x\}$ , is the set of integers for which  $|x| = x$ . Because  $|x| = x$  if and only if  $x \geq 0$ , it follows that the truth set of  $R$  is  $\mathbf{N}$ , the set of nonnegative integers. 

Note that  $\forall x P(x)$  is true over the domain  $U$  if and only if the truth set of  $P$  is the set  $U$ . Likewise,  $\exists x P(x)$  is true over the domain  $U$  if and only if the truth set of  $P$  is nonempty.

## Exercises

- List the members of these sets.
  - $\{x \mid x \text{ is a real number such that } x^2 = 1\}$
  - $\{x \mid x \text{ is a positive integer less than } 12\}$
  - $\{x \mid x \text{ is the square of an integer and } x < 100\}$
  - $\{x \mid x \text{ is an integer such that } x^2 = 2\}$
- Use set builder notation to give a description of each of these sets.
  - $\{0, 3, 6, 9, 12\}$
  - $\{-3, -2, -1, 0, 1, 2, 3\}$
  - $\{m, n, o, p\}$
- For each of these pairs of sets, determine whether the first is a subset of the second, the second is a subset of the first, or neither is a subset of the other.
  - the set of airline flights from New York to New Delhi, the set of nonstop airline flights from New York to New Delhi
  - the set of people who speak English, the set of people who speak Chinese
  - the set of flying squirrels, the set of living creatures that can fly
- For each of these pairs of sets, determine whether the first is a subset of the second, the second is a subset of the first, or neither is a subset of the other.
  - the set of people who speak English, the set of people who speak English with an Australian accent
  - the set of fruits, the set of citrus fruits
  - the set of students studying discrete mathematics, the set of students studying data structures
- Determine whether each of these pairs of sets are equal.
  - $\{1, 3, 3, 3, 5, 5, 5, 5, 5\}$ ,  $\{5, 3, 1\}$
  - $\{\{1\}\}$ ,  $\{1, \{1\}\}$
  - $\emptyset$ ,  $\{\emptyset\}$
- Suppose that  $A = \{2, 4, 6\}$ ,  $B = \{2, 6\}$ ,  $C = \{4, 6\}$ , and  $D = \{4, 6, 8\}$ . Determine which of these sets are subsets of which other of these sets.
- For each of the following sets, determine whether 2 is an element of that set.
  - $\{x \in \mathbf{R} \mid x \text{ is an integer greater than } 1\}$
  - $\{x \in \mathbf{R} \mid x \text{ is the square of an integer}\}$
  - $\{2, \{2\}\}$
  - $\{\{2\}, \{\{2\}\}\}$
  - $\{\{2\}, \{2, \{2\}\}\}$
  - $\{\{\{2\}\}\}$
- For each of the sets in Exercise 7, determine whether  $\{2\}$  is an element of that set.
- Determine whether each of these statements is true or false.
  - $0 \in \emptyset$
  - $\emptyset \in \{0\}$
  - $\{0\} \subset \emptyset$
  - $\emptyset \subset \{0\}$
  - $\{0\} \in \{0\}$
  - $\{0\} \subset \{0\}$
  - $\{\emptyset\} \subseteq \{\emptyset\}$
- Determine whether these statements are true or false.
  - $\emptyset \in \{0\}$
  - $\emptyset \in \{\emptyset, \{\emptyset\}\}$
  - $\{\emptyset\} \in \{0\}$
  - $\{\emptyset\} \in \{\{\emptyset\}\}$
  - $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$
  - $\{\{\emptyset\}\} \subset \{\{\emptyset\}, \{\emptyset\}\}$
- Determine whether each of these statements is true or false.
  - $x \in \{x\}$
  - $\{x\} \subseteq \{x\}$
  - $\{x\} \in \{x\}$
  - $\{x\} \in \{\{x\}\}$
  - $\emptyset \subseteq \{x\}$
  - $\emptyset \in \{x\}$
- Use a Venn diagram to illustrate the subset of odd integers in the set of all positive integers not exceeding 10.

13. Use a Venn diagram to illustrate the set of all months of the year whose names do not contain the letter  $R$  in the set of all months of the year.
14. Use a Venn diagram to illustrate the relationship  $A \subseteq B$  and  $B \subseteq C$ .
15. Use a Venn diagram to illustrate the relationships  $A \subset B$  and  $B \subset C$ .
16. Use a Venn diagram to illustrate the relationships  $A \subset B$  and  $A \subset C$ .
17. Suppose that  $A$ ,  $B$ , and  $C$  are sets such that  $A \subseteq B$  and  $B \subseteq C$ . Show that  $A \subseteq C$ .
18. Find two sets  $A$  and  $B$  such that  $A \in B$  and  $A \subseteq B$ .
19. What is the cardinality of each of these sets?
- $\{a\}$
  - $\{\{a\}\}$
  - $\{a, \{a\}\}$
  - $\{a, \{a\}, \{a, \{a\}\}\}$
20. What is the cardinality of each of these sets?
- $\emptyset$
  - $\{\emptyset\}$
  - $\{\emptyset, \{\emptyset\}\}$
  - $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
21. Find the power set of each of these sets, where  $a$  and  $b$  are distinct elements.
- $\{a\}$
  - $\{a, b\}$
  - $\{\emptyset, \{\emptyset\}\}$
22. Can you conclude that  $A = B$  if  $A$  and  $B$  are two sets with the same power set?
23. How many elements does each of these sets have where  $a$  and  $b$  are distinct elements?
- $\mathcal{P}(\{a, b, \{a, b\}\})$
  - $\mathcal{P}(\{\emptyset, a, \{a\}, \{\{a\}\}\})$
  - $\mathcal{P}(\mathcal{P}(\emptyset))$
24. Determine whether each of these sets is the power set of a set, where  $a$  and  $b$  are distinct elements.
- $\emptyset$
  - $\{\emptyset, \{a\}\}$
  - $\{\emptyset, \{a\}, \{\emptyset, a\}\}$
  - $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
25. Prove that  $\mathcal{P}(A) \subseteq \mathcal{P}(B)$  if and only if  $A \subseteq B$ .
26. Show that if  $A \subseteq C$  and  $B \subseteq D$ , then  $A \times B \subseteq C \times D$ .
27. Let  $A = \{a, b, c, d\}$  and  $B = \{y, z\}$ . Find
- $A \times B$ .
  - $B \times A$ .
28. What is the Cartesian product  $A \times B$ , where  $A$  is the set of courses offered by the mathematics department at a university and  $B$  is the set of mathematics professors at this university? Give an example of how this Cartesian product can be used.
29. What is the Cartesian product  $A \times B \times C$ , where  $A$  is the set of all airlines and  $B$  and  $C$  are both the set of all cities in the United States? Give an example of how this Cartesian product can be used.
30. Suppose that  $A \times B = \emptyset$ , where  $A$  and  $B$  are sets. What can you conclude?
31. Let  $A$  be a set. Show that  $\emptyset \times A = A \times \emptyset = \emptyset$ .
32. Let  $A = \{a, b, c\}$ ,  $B = \{x, y\}$ , and  $C = \{0, 1\}$ . Find
- $A \times B \times C$ .
  - $C \times B \times A$ .
  - $C \times A \times B$ .
  - $B \times B \times B$ .
33. Find  $A^2$  if
- $A = \{0, 1, 3\}$ .
  - $A = \{1, 2, a, b\}$ .
34. Find  $A^3$  if
- $A = \{a\}$ .
  - $A = \{0, a\}$ .
35. How many different elements does  $A \times B$  have if  $A$  has  $m$  elements and  $B$  has  $n$  elements?
36. How many different elements does  $A \times B \times C$  have if  $A$  has  $m$  elements,  $B$  has  $n$  elements, and  $C$  has  $p$  elements?
37. How many different elements does  $A^n$  have when  $A$  has  $m$  elements and  $n$  is a positive integer?
38. Show that  $A \times B \neq B \times A$ , when  $A$  and  $B$  are nonempty, unless  $A = B$ .
39. Explain why  $A \times B \times C$  and  $(A \times B) \times C$  are not the same.
40. Explain why  $(A \times B) \times (C \times D)$  and  $A \times (B \times C) \times D$  are not the same.
41. Translate each of these quantifications into English and determine its truth value.
- $\forall x \in \mathbf{R} (x^2 \neq -1)$
  - $\exists x \in \mathbf{Z} (x^2 = 2)$
  - $\forall x \in \mathbf{Z} (x^2 > 0)$
  - $\exists x \in \mathbf{R} (x^2 = x)$
42. Translate each of these quantifications into English and determine its truth value.
- $\exists x \in \mathbf{R} (x^3 = -1)$
  - $\exists x \in \mathbf{Z} (x + 1 > x)$
  - $\forall x \in \mathbf{Z} (x - 1 \in \mathbf{Z})$
  - $\forall x \in \mathbf{Z} (x^2 \in \mathbf{Z})$
43. Find the truth set of each of these predicates where the domain is the set of integers.
- $P(x): x^2 < 3$
  - $Q(x): x^2 > x$
  - $R(x): 2x + 1 = 0$
44. Find the truth set of each of these predicates where the domain is the set of integers.
- $P(x): x^3 \geq 1$
  - $Q(x): x^2 = 2$
  - $R(x): x < x^2$
- \*45. The defining property of an ordered pair is that two ordered pairs are equal if and only if their first elements are equal and their second elements are equal. Surprisingly, instead of taking the ordered pair as a primitive concept, we can construct ordered pairs using basic notions from set theory. Show that if we define the ordered pair  $(a, b)$  to be  $\{\{a\}, \{a, b\}\}$ , then  $(a, b) = (c, d)$  if and only if  $a = c$  and  $b = d$ . [Hint: First show that  $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$  if and only if  $a = c$  and  $b = d$ .]
- \*46. This exercise presents **Russell's paradox**. Let  $S$  be the set that contains a set  $x$  if the set  $x$  does not belong to itself, so that  $S = \{x \mid x \notin x\}$ .
- Show the assumption that  $S$  is a member of  $S$  leads to a contradiction.
  - Show the assumption that  $S$  is not a member of  $S$  leads to a contradiction.
- By parts (a) and (b) it follows that the set  $S$  cannot be defined as it was. This paradox can be avoided by restricting the types of elements that sets can have.
- \*47. Describe a procedure for listing all the subsets of a finite set.

## Exercises

- Let  $A$  be the set of students who live within one mile of school and let  $B$  be the set of students who walk to classes. Describe the students in each of these sets.
    - $A \cap B$
    - $A \cup B$
    - $A - B$
    - $B - A$
  - Suppose that  $A$  is the set of sophomores at your school and  $B$  is the set of students in discrete mathematics at your school. Express each of these sets in terms of  $A$  and  $B$ .
    - the set of sophomores taking discrete mathematics in your school
    - the set of sophomores at your school who are not taking discrete mathematics
    - the set of students at your school who either are sophomores or are taking discrete mathematics
    - the set of students at your school who either are not sophomores or are not taking discrete mathematics
  - Let  $A = \{1, 2, 3, 4, 5\}$  and  $B = \{0, 3, 6\}$ . Find
    - $A \cup B$
    - $A \cap B$
    - $A - B$
    - $B - A$
  - Let  $A = \{a, b, c, d, e\}$  and  $B = \{a, b, c, d, e, f, g, h\}$ . Find
    - $A \cup B$
    - $A \cap B$
    - $A - B$
    - $B - A$
- In Exercises 5–10 assume that  $A$  is a subset of some underlying universal set  $U$ .
- Prove the complementation law in Table 1 by showing that  $\overline{\overline{A}} = A$ .
  - Prove the identity laws in Table 1 by showing that
    - $A \cup \emptyset = A$
    - $A \cap U = A$
  - Prove the domination laws in Table 1 by showing that
    - $A \cup U = U$
    - $A \cap \emptyset = \emptyset$
  - Prove the idempotent laws in Table 1 by showing that
    - $A \cup A = A$
    - $A \cap A = A$
  - Prove the complement laws in Table 1 by showing that
    - $A \cup \overline{A} = U$
    - $A \cap \overline{A} = \emptyset$
  - Show that
    - $A - \emptyset = A$
    - $\emptyset - A = \emptyset$
  - Let  $A$  and  $B$  be sets. Prove the commutative laws from Table 1 by showing that
    - $A \cup B = B \cup A$
    - $A \cap B = B \cap A$
  - Prove the first absorption law from Table 1 by showing that if  $A$  and  $B$  are sets, then  $A \cup (A \cap B) = A$ .
  - Prove the second absorption law from Table 1 by showing that if  $A$  and  $B$  are sets, then  $A \cap (A \cup B) = A$ .
  - Find the sets  $A$  and  $B$  if  $A - B = \{1, 5, 7, 8\}$ ,  $B - A = \{2, 10\}$ , and  $A \cap B = \{3, 6, 9\}$ .
  - Prove the second De Morgan law in Table 1 by showing that if  $A$  and  $B$  are sets, then  $\overline{A \cup B} = \overline{A} \cap \overline{B}$ 
    - by showing each side is a subset of the other side.
    - using a membership table.
  - Let  $A$  and  $B$  be sets. Show that
    - $(A \cap B) \subseteq A$
    - $A \subseteq (A \cup B)$
    - $A - B \subseteq A$
    - $A \cap (B - A) = \emptyset$
    - $A \cup (B - A) = A \cup B$
  - Show that if  $A$ ,  $B$ , and  $C$  are sets, then  $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$ 
    - by showing each side is a subset of the other side.
    - using a membership table.
  - Let  $A$ ,  $B$ , and  $C$  be sets. Show that
    - $(A \cup B) \subseteq (A \cup B \cup C)$
    - $(A \cap B \cap C) \subseteq (A \cap B)$
    - $(A - B) - C \subseteq A - C$
    - $(A - C) \cap (C - B) = \emptyset$
    - $(B - A) \cup (C - A) = (B \cup C) - A$
  - Show that if  $A$  and  $B$  are sets, then
    - $A - B = A \cap \overline{B}$
    - $(A \cap B) \cup (A \cap \overline{B}) = A$
  - Show that if  $A$  and  $B$  are sets with  $A \subseteq B$ , then
    - $A \cup B = B$
    - $A \cap B = A$
  - Prove the first associative law from Table 1 by showing that if  $A$ ,  $B$ , and  $C$  are sets, then  $A \cup (B \cup C) = (A \cup B) \cup C$ .
  - Prove the second associative law from Table 1 by showing that if  $A$ ,  $B$ , and  $C$  are sets, then  $A \cap (B \cap C) = (A \cap B) \cap C$ .
  - Prove the first distributive law from Table 1 by showing that if  $A$ ,  $B$ , and  $C$  are sets, then  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .
  - Let  $A$ ,  $B$ , and  $C$  be sets. Show that  $(A - B) - C = (A - C) - (B - C)$ .
  - Let  $A = \{0, 2, 4, 6, 8, 10\}$ ,  $B = \{0, 1, 2, 3, 4, 5, 6\}$ , and  $C = \{4, 5, 6, 7, 8, 9, 10\}$ . Find
    - $A \cap B \cap C$
    - $A \cup B \cup C$
    - $(A \cup B) \cap C$
    - $(A \cap B) \cup C$
  - Draw the Venn diagrams for each of these combinations of the sets  $A$ ,  $B$ , and  $C$ .
    - $A \cap (B \cup C)$
    - $\overline{A} \cap \overline{B} \cap \overline{C}$
    - $(A - B) \cup (A - C) \cup (B - C)$
  - Draw the Venn diagrams for each of these combinations of the sets  $A$ ,  $B$ , and  $C$ .
    - $A \cap (B - C)$
    - $(A \cap B) \cup (A \cap C)$
    - $(A \cap \overline{B}) \cup (A \cap \overline{C})$
  - Draw the Venn diagrams for each of these combinations of the sets  $A$ ,  $B$ ,  $C$ , and  $D$ .
    - $(A \cap B) \cup (C \cap D)$
    - $\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}$
    - $A - (B \cap C \cap D)$
  - What can you say about the sets  $A$  and  $B$  if we know that
    - $A \cup B = A$
    - $A \cap B = A$
    - $A - B = A$
    - $A \cap B = B \cap A$
    - $A - B = B - A$

30. Can you conclude that  $A = B$  if  $A$ ,  $B$ , and  $C$  are sets such that
- $A \cup C = B \cup C$ ?
  - $A \cap C = B \cap C$ ?
  - $A \cup C = B \cup C$  and  $A \cap C = B \cap C$ ?
31. Let  $A$  and  $B$  be subsets of a universal set  $U$ . Show that  $A \subseteq B$  if and only if  $\overline{B} \subseteq \overline{A}$ .
- The **symmetric difference** of  $A$  and  $B$ , denoted by  $A \oplus B$ , is the set containing those elements in either  $A$  or  $B$ , but not in both  $A$  and  $B$ .
32. Find the symmetric difference of  $\{1, 3, 5\}$  and  $\{1, 2, 3\}$ .
33. Find the symmetric difference of the set of computer science majors at a school and the set of mathematics majors at this school.
34. Draw a Venn diagram for the symmetric difference of the sets  $A$  and  $B$ .
35. Show that  $A \oplus B = (A \cup B) - (A \cap B)$ .
36. Show that  $A \oplus B = (A - B) \cup (B - A)$ .
37. Show that if  $A$  is a subset of a universal set  $U$ , then
- $A \oplus A = \emptyset$ .
  - $A \oplus \emptyset = A$ .
  - $A \oplus U = \overline{A}$ .
  - $A \oplus \overline{A} = U$ .
38. Show that if  $A$  and  $B$  are sets, then
- $A \oplus B = B \oplus A$ .
  - $(A \oplus B) \oplus B = A$ .
39. What can you say about the sets  $A$  and  $B$  if  $A \oplus B = A$ ?
- \*40. Determine whether the symmetric difference is associative; that is, if  $A$ ,  $B$ , and  $C$  are sets, does it follow that  $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ ?
- \*41. Suppose that  $A$ ,  $B$ , and  $C$  are sets such that  $A \oplus C = B \oplus C$ . Must it be the case that  $A = B$ ?
42. If  $A$ ,  $B$ ,  $C$ , and  $D$  are sets, does it follow that  $(A \oplus B) \oplus (C \oplus D) = (A \oplus C) \oplus (B \oplus D)$ ?
43. If  $A$ ,  $B$ ,  $C$ , and  $D$  are sets, does it follow that  $(A \oplus B) \oplus (C \oplus D) = (A \oplus D) \oplus (B \oplus C)$ ?
44. Show that if  $A$  and  $B$  are finite sets, then  $A \cup B$  is a finite set.
45. Show that if  $A$  is an infinite set, then whenever  $B$  is a set,  $A \cup B$  is also an infinite set.
- \*46. Show that if  $A$ ,  $B$ , and  $C$  are sets, then
- $$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$
- (This is a special case of the inclusion–exclusion principle, which will be studied in Chapter 8.)
47. Let  $A_i = \{1, 2, 3, \dots, i\}$  for  $i = 1, 2, 3, \dots$ . Find
- $\bigcup_{i=1}^n A_i$ .
  - $\bigcap_{i=1}^n A_i$ .
48. Let  $A_i = \{\dots, -2, -1, 0, 1, \dots, i\}$ . Find
- $\bigcup_{i=1}^n A_i$ .
  - $\bigcap_{i=1}^n A_i$ .
49. Let  $A_i$  be the set of all nonempty bit strings (that is, bit strings of length at least one) of length not exceeding  $i$ . Find
- $\bigcup_{i=1}^n A_i$ .
  - $\bigcap_{i=1}^n A_i$ .
50. Find  $\bigcup_{i=1}^{\infty} A_i$  and  $\bigcap_{i=1}^{\infty} A_i$  if for every positive integer  $i$ ,
- $A_i = \{i, i+1, i+2, \dots\}$ .
  - $A_i = \{0, i\}$ .
  - $A_i = (0, i)$ , that is, the set of real numbers  $x$  with  $0 < x < i$ .
  - $A_i = (i, \infty)$ , that is, the set of real numbers  $x$  with  $x > i$ .
51. Find  $\bigcup_{i=1}^{\infty} A_i$  and  $\bigcap_{i=1}^{\infty} A_i$  if for every positive integer  $i$ ,
- $A_i = \{-i, -i+1, \dots, -1, 0, 1, \dots, i-1, i\}$ .
  - $A_i = \{-i, i\}$ .
  - $A_i = [-i, i]$ , that is, the set of real numbers  $x$  with  $-i \leq x \leq i$ .
  - $A_i = [i, \infty)$ , that is, the set of real numbers  $x$  with  $x \geq i$ .
52. Suppose that the universal set is  $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ . Express each of these sets with bit strings where the  $i$ th bit in the string is 1 if  $i$  is in the set and 0 otherwise.
- $\{3, 4, 5\}$
  - $\{1, 3, 6, 10\}$
  - $\{2, 3, 4, 7, 8, 9\}$
53. Using the same universal set as in the last problem, find the set specified by each of these bit strings.
- 11 1100 1111
  - 01 0111 1000
  - 10 0000 0001
54. What subsets of a finite universal set do these bit strings represent?
- the string with all zeros
  - the string with all ones
55. What is the bit string corresponding to the difference of two sets?
56. What is the bit string corresponding to the symmetric difference of two sets?
57. Show how bitwise operations on bit strings can be used to find these combinations of  $A = \{a, b, c, d, e\}$ ,  $B = \{b, c, d, g, p, t, v\}$ ,  $C = \{c, e, i, o, u, x, y, z\}$ , and  $D = \{d, e, h, i, n, o, t, u, x, y\}$ .
- $A \cup B$
  - $A \cap B$
  - $(A \cup D) \cap (B \cup C)$
  - $A \cup B \cup C \cup D$
58. How can the union and intersection of  $n$  sets that all are subsets of the universal set  $U$  be found using bit strings?
- The **successor** of the set  $A$  is the set  $A \cup \{A\}$ .
59. Find the successors of the following sets.
- $\{1, 2, 3\}$
  - $\emptyset$
  - $\{\emptyset\}$
  - $\{\emptyset, \{\emptyset\}\}$



60. How many elements does the successor of a set with  $n$  elements have?

Sometimes the number of times that an element occurs in an unordered collection matters. **Multisets** are unordered collections of elements where an element can occur as a member more than once. The notation  $\{m_1 \cdot a_1, m_2 \cdot a_2, \dots, m_r \cdot a_r\}$  denotes the multiset with element  $a_1$  occurring  $m_1$  times, element  $a_2$  occurring  $m_2$  times, and so on. The numbers  $m_i$ ,  $i = 1, 2, \dots, r$  are called the **multiplicities** of the elements  $a_i$ ,  $i = 1, 2, \dots, r$ .

Let  $P$  and  $Q$  be multisets. The **union** of the multisets  $P$  and  $Q$  is the multiset where the multiplicity of an element is the maximum of its multiplicities in  $P$  and  $Q$ . The **intersection** of  $P$  and  $Q$  is the multiset where the multiplicity of an element is the minimum of its multiplicities in  $P$  and  $Q$ . The **difference** of  $P$  and  $Q$  is the multiset where the multiplicity of an element is the multiplicity of the element in  $P$  less its multiplicity in  $Q$  unless this difference is negative, in which case the multiplicity is 0. The **sum** of  $P$  and  $Q$  is the multiset where the multiplicity of an element is the sum of multiplicities in  $P$  and  $Q$ . The union, intersection, and difference of  $P$  and  $Q$  are denoted by  $P \cup Q$ ,  $P \cap Q$ , and  $P - Q$ , respectively (where these operations should not be confused with the analogous operations for sets). The sum of  $P$  and  $Q$  is denoted by  $P + Q$ .

61. Let  $A$  and  $B$  be the multisets  $\{3 \cdot a, 2 \cdot b, 1 \cdot c\}$  and  $\{2 \cdot a, 3 \cdot b, 4 \cdot d\}$ , respectively. Find
- a)  $A \cup B$ .      b)  $A \cap B$ .      c)  $A - B$ .  
 d)  $B - A$ .      e)  $A + B$ .
62. Suppose that  $A$  is the multiset that has as its elements the types of computer equipment needed by one department of a university and the multiplicities are the number of pieces of each type needed, and  $B$  is the analogous multiset for a second department of the university. For instance,  $A$  could be the multiset  $\{107 \cdot \text{personal computers}, 44 \cdot \text{routers}, 6 \cdot \text{servers}\}$  and  $B$  could be the multiset  $\{14 \cdot \text{personal computers}, 6 \cdot \text{routers}, 2 \cdot \text{mainframes}\}$ .
- a) What combination of  $A$  and  $B$  represents the equipment the university should buy assuming both departments use the same equipment?

- b) What combination of  $A$  and  $B$  represents the equipment that will be used by both departments if both departments use the same equipment?
- c) What combination of  $A$  and  $B$  represents the equipment that the second department uses, but the first department does not, if both departments use the same equipment?
- d) What combination of  $A$  and  $B$  represents the equipment that the university should purchase if the departments do not share equipment?

**Fuzzy sets** are used in artificial intelligence. Each element in the universal set  $U$  has a **degree of membership**, which is a real number between 0 and 1 (including 0 and 1), in a fuzzy set  $S$ . The fuzzy set  $S$  is denoted by listing the elements with their degrees of membership (elements with 0 degree of membership are not listed). For instance, we write  $\{0.6 \text{ Alice}, 0.9 \text{ Brian}, 0.4 \text{ Fred}, 0.1 \text{ Oscar}, 0.5 \text{ Rita}\}$  for the set  $F$  (of famous people) to indicate that Alice has a 0.6 degree of membership in  $F$ , Brian has a 0.9 degree of membership in  $F$ , Fred has a 0.4 degree of membership in  $F$ , Oscar has a 0.1 degree of membership in  $F$ , and Rita has a 0.5 degree of membership in  $F$  (so that Brian is the most famous and Oscar is the least famous of these people). Also suppose that  $R$  is the set of rich people with  $R = \{0.4 \text{ Alice}, 0.8 \text{ Brian}, 0.2 \text{ Fred}, 0.9 \text{ Oscar}, 0.7 \text{ Rita}\}$ .

63. The **complement** of a fuzzy set  $S$  is the set  $\bar{S}$ , with the degree of the membership of an element in  $\bar{S}$  equal to 1 minus the degree of membership of this element in  $S$ . Find  $\bar{F}$  (the fuzzy set of people who are not famous) and  $\bar{R}$  (the fuzzy set of people who are not rich).
64. The **union** of two fuzzy sets  $S$  and  $T$  is the fuzzy set  $S \cup T$ , where the degree of membership of an element in  $S \cup T$  is the maximum of the degrees of membership of this element in  $S$  and in  $T$ . Find the fuzzy set  $F \cup R$  of rich or famous people.
65. The **intersection** of two fuzzy sets  $S$  and  $T$  is the fuzzy set  $S \cap T$ , where the degree of membership of an element in  $S \cap T$  is the minimum of the degrees of membership of this element in  $S$  and in  $T$ . Find the fuzzy set  $F \cap R$  of rich and famous people.

## 2.3 Functions

### Introduction

In many instances we assign to each element of a set a particular element of a second set (which may be the same as the first). For example, suppose that each student in a discrete mathematics class is assigned a letter grade from the set  $\{A, B, C, D, F\}$ . And suppose that the grades are  $A$  for Adams,  $C$  for Chou,  $B$  for Goodfriend,  $A$  for Rodriguez, and  $F$  for Stevens. This assignment of grades is illustrated in Figure 1.

This assignment is an example of a function. The concept of a function is extremely important in mathematics and computer science. For example, in discrete mathematics functions are used in the definition of such discrete structures as sequences and strings. Functions are also used to represent how long it takes a computer to solve problems of a given size. Many computer programs and subroutines are designed to calculate values of functions. Recursive functions,

## Partial Functions

A program designed to evaluate a function may not produce the correct value of the function for all elements in the domain of this function. For example, a program may not produce a correct value because evaluating the function may lead to an infinite loop or an overflow. Similarly, in abstract mathematics, we often want to discuss functions that are defined only for a subset of the real numbers, such as  $1/x$ ,  $\sqrt{x}$ , and  $\arcsin(x)$ . Also, we may want to use such notions as the “youngest child” function, which is undefined for a couple having no children, or the “time of sunrise,” which is undefined for some days above the Arctic Circle. To study such situations, we use the concept of a partial function.

### DEFINITION 13

A *partial function*  $f$  from a set  $A$  to a set  $B$  is an assignment to each element  $a$  in a subset of  $A$ , called the *domain of definition* of  $f$ , of a unique element  $b$  in  $B$ . The sets  $A$  and  $B$  are called the *domain* and *codomain* of  $f$ , respectively. We say that  $f$  is *undefined* for elements in  $A$  that are not in the domain of definition of  $f$ . When the domain of definition of  $f$  equals  $A$ , we say that  $f$  is a *total function*.

**Remark:** We write  $f : A \rightarrow B$  to denote that  $f$  is a partial function from  $A$  to  $B$ . Note that this is the same notation as is used for functions. The context in which the notation is used determines whether  $f$  is a partial function or a total function.

### EXAMPLE 32

The function  $f : \mathbf{Z} \rightarrow \mathbf{R}$  where  $f(n) = \sqrt{n}$  is a partial function from  $\mathbf{Z}$  to  $\mathbf{R}$  where the domain of definition is the set of nonnegative integers. Note that  $f$  is undefined for negative integers. ◀

## Exercises

- Why is  $f$  not a function from  $\mathbf{R}$  to  $\mathbf{R}$  if
  - $f(x) = 1/x$ ?
  - $f(x) = \sqrt{x}$ ?
  - $f(x) = \pm\sqrt{(x^2 + 1)}$ ?
- Determine whether  $f$  is a function from  $\mathbf{Z}$  to  $\mathbf{R}$  if
  - $f(n) = \pm n$ .
  - $f(n) = \sqrt{n^2 + 1}$ .
  - $f(n) = 1/(n^2 - 4)$ .
- Determine whether  $f$  is a function from the set of all bit strings to the set of integers if
  - $f(S)$  is the position of a 0 bit in  $S$ .
  - $f(S)$  is the number of 1 bits in  $S$ .
  - $f(S)$  is the smallest integer  $i$  such that the  $i$ th bit of  $S$  is 1 and  $f(S) = 0$  when  $S$  is the empty string, the string with no bits.
- Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.
  - the function that assigns to each nonnegative integer its last digit
  - the function that assigns the next largest integer to a positive integer
  - the function that assigns to a bit string the number of one bits in the string
  - the function that assigns to a bit string the number of bits in the string
- Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.
  - the function that assigns to each bit string the number of ones in the string minus the number of zeros in the string
  - the function that assigns to each bit string twice the number of zeros in that string
  - the function that assigns the number of bits left over when a bit string is split into bytes (which are blocks of 8 bits)
  - the function that assigns to each positive integer the largest perfect square not exceeding this integer
- Find the domain and range of these functions.
  - the function that assigns to each pair of positive integers the first integer of the pair
  - the function that assigns to each positive integer its largest decimal digit
  - the function that assigns to a bit string the number of ones minus the number of zeros in the string
  - the function that assigns to each positive integer the largest integer not exceeding the square root of the integer
  - the function that assigns to a bit string the longest string of ones in the string

7. Find the domain and range of these functions.
  - a) the function that assigns to each pair of positive integers the maximum of these two integers
  - b) the function that assigns to each positive integer the number of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 that do not appear as decimal digits of the integer
  - c) the function that assigns to a bit string the number of times the block 11 appears
  - d) the function that assigns to a bit string the numerical position of the first 1 in the string and that assigns the value 0 to a bit string consisting of all 0s
8. Find these values.
 

a) $\lfloor 1.1 \rfloor$	b) $\lceil 1.1 \rceil$
c) $\lfloor -0.1 \rfloor$	d) $\lceil -0.1 \rceil$
e) $\lceil 2.99 \rceil$	f) $\lfloor -2.99 \rfloor$
g) $\lfloor \frac{1}{2} \rfloor + \lceil \frac{1}{2} \rceil$	h) $\lceil \lfloor \frac{1}{2} \rfloor \rceil + \lceil \frac{1}{2} \rceil + \frac{1}{2}$
9. Find these values.
 

a) $\lceil \frac{3}{4} \rceil$	b) $\lfloor \frac{7}{8} \rfloor$
c) $\lceil -\frac{3}{4} \rceil$	d) $\lfloor -\frac{7}{8} \rfloor$
e) $\lceil 3 \rceil$	f) $\lfloor -1 \rfloor$
g) $\lfloor \frac{1}{2} \rfloor + \lceil \frac{3}{2} \rceil$	h) $\lfloor \frac{1}{2} \rfloor \cdot \lfloor \frac{5}{2} \rfloor$
10. Determine whether each of these functions from  $\{a, b, c, d\}$  to itself is one-to-one.
  - a)  $f(a) = b, f(b) = a, f(c) = c, f(d) = d$
  - b)  $f(a) = b, f(b) = b, f(c) = d, f(d) = c$
  - c)  $f(a) = d, f(b) = b, f(c) = c, f(d) = d$
11. Which functions in Exercise 10 are onto?
12. Determine whether each of these functions from  $\mathbf{Z}$  to  $\mathbf{Z}$  is one-to-one.
 

a) $f(n) = n - 1$	b) $f(n) = n^2 + 1$
c) $f(n) = n^3$	d) $f(n) = \lceil n/2 \rceil$
13. Which functions in Exercise 12 are onto?
14. Determine whether  $f: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$  is onto if
  - a)  $f(m, n) = 2m - n.$
  - b)  $f(m, n) = m^2 - n^2.$
  - c)  $f(m, n) = m + n + 1.$
  - d)  $f(m, n) = |m| - |n|.$
  - e)  $f(m, n) = m^2 - 4.$
15. Determine whether the function  $f: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$  is onto if
  - a)  $f(m, n) = m + n.$
  - b)  $f(m, n) = m^2 + n^2.$
  - c)  $f(m, n) = m.$
  - d)  $f(m, n) = |n|.$
  - e)  $f(m, n) = m - n.$
16. Consider these functions from the set of students in a discrete mathematics class. Under what conditions is the function one-to-one if it assigns to a student his or her
  - a) mobile phone number.
  - b) student identification number.
  - c) final grade in the class.
  - d) home town.
17. Consider these functions from the set of teachers in a school. Under what conditions is the function one-to-one if it assigns to a teacher his or her
  - a) office.
  - b) assigned bus to chaperone in a group of buses taking students on a field trip.
  - c) salary.
  - d) social security number.
18. Specify a codomain for each of the functions in Exercise 16. Under what conditions is each of these functions with the codomain you specified onto?
19. Specify a codomain for each of the functions in Exercise 17. Under what conditions is each of the functions with the codomain you specified onto?
20. Give an example of a function from  $\mathbf{N}$  to  $\mathbf{N}$  that is
  - a) one-to-one but not onto.
  - b) onto but not one-to-one.
  - c) both onto and one-to-one (but different from the identity function).
  - d) neither one-to-one nor onto.
21. Give an explicit formula for a function from the set of integers to the set of positive integers that is
  - a) one-to-one, but not onto.
  - b) onto, but not one-to-one.
  - c) one-to-one and onto.
  - d) neither one-to-one nor onto.
22. Determine whether each of these functions is a bijection from  $\mathbf{R}$  to  $\mathbf{R}$ .
  - a)  $f(x) = -3x + 4$
  - b)  $f(x) = -3x^2 + 7$
  - c)  $f(x) = (x + 1)/(x + 2)$
  - d)  $f(x) = x^5 + 1$
23. Determine whether each of these functions is a bijection from  $\mathbf{R}$  to  $\mathbf{R}$ .
  - a)  $f(x) = 2x + 1$
  - b)  $f(x) = x^2 + 1$
  - c)  $f(x) = x^3$
  - d)  $f(x) = (x^2 + 1)/(x^2 + 2)$
24. Let  $f: \mathbf{R} \rightarrow \mathbf{R}$  and let  $f(x) > 0$  for all  $x \in \mathbf{R}$ . Show that  $f(x)$  is strictly increasing if and only if the function  $g(x) = 1/f(x)$  is strictly decreasing.
25. Let  $f: \mathbf{R} \rightarrow \mathbf{R}$  and let  $f(x) > 0$  for all  $x \in \mathbf{R}$ . Show that  $f(x)$  is strictly decreasing if and only if the function  $g(x) = 1/f(x)$  is strictly increasing.
26. a) Prove that a strictly increasing function from  $\mathbf{R}$  to itself is one-to-one.  
 b) Give an example of an increasing function from  $\mathbf{R}$  to itself that is not one-to-one.
27. a) Prove that a strictly decreasing function from  $\mathbf{R}$  to itself is one-to-one.  
 b) Give an example of a decreasing function from  $\mathbf{R}$  to itself that is not one-to-one.
28. Show that the function  $f(x) = e^x$  from the set of real numbers to the set of real numbers is not invertible, but if the codomain is restricted to the set of positive real numbers, the resulting function is invertible.

29. Show that the function  $f(x) = |x|$  from the set of real numbers to the set of nonnegative real numbers is not invertible, but if the domain is restricted to the set of nonnegative real numbers, the resulting function is invertible.
30. Let  $S = \{-1, 0, 2, 4, 7\}$ . Find  $f(S)$  if
- $f(x) = 1$ .
  - $f(x) = 2x + 1$ .
  - $f(x) = \lceil x/5 \rceil$ .
  - $f(x) = \lfloor (x^2 + 1)/3 \rfloor$ .
31. Let  $f(x) = \lfloor x^2/3 \rfloor$ . Find  $f(S)$  if
- $S = \{-2, -1, 0, 1, 2, 3\}$ .
  - $S = \{0, 1, 2, 3, 4, 5\}$ .
  - $S = \{1, 5, 7, 11\}$ .
  - $S = \{2, 6, 10, 14\}$ .
32. Let  $f(x) = 2x$  where the domain is the set of real numbers. What is
- $f(\mathbf{Z})$ ?
  - $f(\mathbf{N})$ ?
  - $f(\mathbf{R})$ ?
33. Suppose that  $g$  is a function from  $A$  to  $B$  and  $f$  is a function from  $B$  to  $C$ .
- Show that if both  $f$  and  $g$  are one-to-one functions, then  $f \circ g$  is also one-to-one.
  - Show that if both  $f$  and  $g$  are onto functions, then  $f \circ g$  is also onto.
- \*34. If  $f$  and  $f \circ g$  are one-to-one, does it follow that  $g$  is one-to-one? Justify your answer.
- \*35. If  $f$  and  $f \circ g$  are onto, does it follow that  $g$  is onto? Justify your answer.
36. Find  $f \circ g$  and  $g \circ f$ , where  $f(x) = x^2 + 1$  and  $g(x) = x + 2$ , are functions from  $\mathbf{R}$  to  $\mathbf{R}$ .
37. Find  $f + g$  and  $fg$  for the functions  $f$  and  $g$  given in Exercise 36.
38. Let  $f(x) = ax + b$  and  $g(x) = cx + d$ , where  $a, b, c$ , and  $d$  are constants. Determine necessary and sufficient conditions on the constants  $a, b, c$ , and  $d$  so that  $f \circ g = g \circ f$ .
39. Show that the function  $f(x) = ax + b$  from  $\mathbf{R}$  to  $\mathbf{R}$  is invertible, where  $a$  and  $b$  are constants, with  $a \neq 0$ , and find the inverse of  $f$ .
40. Let  $f$  be a function from the set  $A$  to the set  $B$ . Let  $S$  and  $T$  be subsets of  $A$ . Show that
- $f(S \cup T) = f(S) \cup f(T)$ .
  - $f(S \cap T) \subseteq f(S) \cap f(T)$ .
41. a) Give an example to show that the inclusion in part (b) in Exercise 40 may be proper.  
b) Show that if  $f$  is one-to-one, the inclusion in part (b) in Exercise 40 is an equality.
- Let  $f$  be a function from the set  $A$  to the set  $B$ . Let  $S$  be a subset of  $B$ . We define the **inverse image** of  $S$  to be the subset of  $A$  whose elements are precisely all pre-images of all elements of  $S$ . We denote the inverse image of  $S$  by  $f^{-1}(S)$ , so  $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$ . (Beware: The notation  $f^{-1}$  is used in two different ways. Do not confuse the notation introduced here with the notation  $f^{-1}(y)$  for the value at  $y$  of the

inverse of the invertible function  $f$ . Notice also that  $f^{-1}(S)$ , the inverse image of the set  $S$ , makes sense for all functions  $f$ , not just invertible functions.)

42. Let  $f$  be the function from  $\mathbf{R}$  to  $\mathbf{R}$  defined by  $f(x) = x^2$ . Find
- $f^{-1}(\{1\})$ .
  - $f^{-1}(\{x \mid 0 < x < 1\})$ .
  - $f^{-1}(\{x \mid x > 4\})$ .
43. Let  $g(x) = \lfloor x \rfloor$ . Find
- $g^{-1}(\{0\})$ .
  - $g^{-1}(\{-1, 0, 1\})$ .
  - $g^{-1}(\{x \mid 0 < x < 1\})$ .
44. Let  $f$  be a function from  $A$  to  $B$ . Let  $S$  and  $T$  be subsets of  $B$ . Show that
- $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$ .
  - $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$ .
45. Let  $f$  be a function from  $A$  to  $B$ . Let  $S$  be a subset of  $B$ . Show that  $f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$ .
46. Show that  $\lfloor x + \frac{1}{2} \rfloor$  is the closest integer to the number  $x$ , except when  $x$  is midway between two integers, when it is the larger of these two integers.
47. Show that  $\lceil x - \frac{1}{2} \rceil$  is the closest integer to the number  $x$ , except when  $x$  is midway between two integers, when it is the smaller of these two integers.
48. Show that if  $x$  is a real number, then  $\lceil x \rceil - \lfloor x \rfloor = 1$  if  $x$  is not an integer and  $\lceil x \rceil - \lfloor x \rfloor = 0$  if  $x$  is an integer.
49. Show that if  $x$  is a real number, then  $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$ .
50. Show that if  $x$  is a real number and  $m$  is an integer, then  $\lceil x + m \rceil = \lceil x \rceil + m$ .
51. Show that if  $x$  is a real number and  $n$  is an integer, then
- $x < n$  if and only if  $\lfloor x \rfloor < n$ .
  - $n < x$  if and only if  $n < \lceil x \rceil$ .
52. Show that if  $x$  is a real number and  $n$  is an integer, then
- $x \leq n$  if and only if  $\lceil x \rceil \leq n$ .
  - $n \leq x$  if and only if  $n \leq \lfloor x \rfloor$ .
53. Prove that if  $n$  is an integer, then  $\lfloor n/2 \rfloor = n/2$  if  $n$  is even and  $(n - 1)/2$  if  $n$  is odd.
54. Prove that if  $x$  is a real number, then  $\lfloor -x \rfloor = -\lceil x \rceil$  and  $\lceil -x \rceil = -\lfloor x \rfloor$ .
55. The function INT is found on some calculators, where  $\text{INT}(x) = \lfloor x \rfloor$  when  $x$  is a nonnegative real number and  $\text{INT}(x) = \lceil x \rceil$  when  $x$  is a negative real number. Show that this INT function satisfies the identity  $\text{INT}(-x) = -\text{INT}(x)$ .
56. Let  $a$  and  $b$  be real numbers with  $a < b$ . Use the floor and/or ceiling functions to express the number of integers  $n$  that satisfy the inequality  $a \leq n \leq b$ .
57. Let  $a$  and  $b$  be real numbers with  $a < b$ . Use the floor and/or ceiling functions to express the number of integers  $n$  that satisfy the inequality  $a < n < b$ .
58. How many bytes are required to encode  $n$  bits of data where  $n$  equals
- 4?
  - 10?
  - 500?
  - 3000?

59. How many bytes are required to encode  $n$  bits of data where  $n$  equals  
 a) 7?      b) 17?      c) 1001?      d) 28,800?
60. How many ATM cells (described in Example 28) can be transmitted in 10 seconds over a link operating at the following rates?  
 a) 128 kilobits per second (1 kilobit = 1000 bits)  
 b) 300 kilobits per second  
 c) 1 megabit per second (1 megabit = 1,000,000 bits)
61. Data are transmitted over a particular Ethernet network in blocks of 1500 octets (blocks of 8 bits). How many blocks are required to transmit the following amounts of data over this Ethernet network? (Note that a byte is a synonym for an octet, a kilobyte is 1000 bytes, and a megabyte is 1,000,000 bytes.)  
 a) 150 kilobytes of data  
 b) 384 kilobytes of data  
 c) 1.544 megabytes of data  
 d) 45.3 megabytes of data
62. Draw the graph of the function  $f(n) = 1 - n^2$  from  $\mathbf{Z}$  to  $\mathbf{Z}$ .
63. Draw the graph of the function  $f(x) = \lfloor 2x \rfloor$  from  $\mathbf{R}$  to  $\mathbf{R}$ .
64. Draw the graph of the function  $f(x) = \lfloor x/2 \rfloor$  from  $\mathbf{R}$  to  $\mathbf{R}$ .
65. Draw the graph of the function  $f(x) = \lfloor x \rfloor + \lfloor x/2 \rfloor$  from  $\mathbf{R}$  to  $\mathbf{R}$ .
66. Draw the graph of the function  $f(x) = \lceil x \rceil + \lfloor x/2 \rfloor$  from  $\mathbf{R}$  to  $\mathbf{R}$ .
67. Draw graphs of each of these functions.  
 a)  $f(x) = \lfloor x + \frac{1}{2} \rfloor$       b)  $f(x) = \lfloor 2x + 1 \rfloor$   
 c)  $f(x) = \lceil x/3 \rceil$       d)  $f(x) = \lceil 1/x \rceil$   
 e)  $f(x) = \lceil x - 2 \rceil + \lfloor x + 2 \rfloor$   
 f)  $f(x) = \lfloor 2x \rfloor \lceil x/2 \rceil$       g)  $f(x) = \lceil \lfloor x - \frac{1}{2} \rfloor + \frac{1}{2} \rceil$
68. Draw graphs of each of these functions.  
 a)  $f(x) = \lfloor 3x - 2 \rfloor$       b)  $f(x) = \lceil 0.2x \rceil$   
 c)  $f(x) = \lfloor -1/x \rfloor$       d)  $f(x) = \lfloor x^2 \rfloor$   
 e)  $f(x) = \lceil x/2 \rceil \lfloor x/2 \rfloor$       f)  $f(x) = \lfloor x/2 \rfloor + \lceil x/2 \rceil$   
 g)  $f(x) = \lfloor 2 \lceil x/2 \rceil + \frac{1}{2} \rfloor$
69. Find the inverse function of  $f(x) = x^3 + 1$ .
70. Suppose that  $f$  is an invertible function from  $Y$  to  $Z$  and  $g$  is an invertible function from  $X$  to  $Y$ . Show that the inverse of the composition  $f \circ g$  is given by  $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ .
71. Let  $S$  be a subset of a universal set  $U$ . The **characteristic function**  $f_S$  of  $S$  is the function from  $U$  to the set  $\{0, 1\}$  such that  $f_S(x) = 1$  if  $x$  belongs to  $S$  and  $f_S(x) = 0$  if  $x$  does not belong to  $S$ . Let  $A$  and  $B$  be sets. Show that for all  $x \in U$ ,  
 a)  $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$   
 b)  $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$   
 c)  $f_{\bar{A}}(x) = 1 - f_A(x)$   
 d)  $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x)f_B(x)$
72. Suppose that  $f$  is a function from  $A$  to  $B$ , where  $A$  and  $B$  are finite sets with  $|A| = |B|$ . Show that  $f$  is one-to-one if and only if it is onto.
73. Prove or disprove each of these statements about the floor and ceiling functions.  
 a)  $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$  for all real numbers  $x$ .  
 b)  $\lfloor 2x \rfloor = 2\lfloor x \rfloor$  whenever  $x$  is a real number.  
 c)  $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil = 0$  or  $1$  whenever  $x$  and  $y$  are real numbers.  
 d)  $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$  for all real numbers  $x$  and  $y$ .  
 e)  $\lceil \frac{x}{2} \rceil = \left\lceil \frac{x+1}{2} \right\rceil$  for all real numbers  $x$ .
74. Prove or disprove each of these statements about the floor and ceiling functions.  
 a)  $\lfloor \lceil x \rceil \rfloor = \lceil x \rceil$  for all real numbers  $x$ .  
 b)  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$  for all real numbers  $x$  and  $y$ .  
 c)  $\lceil \lfloor x/2 \rfloor / 2 \rceil = \lceil x/4 \rceil$  for all real numbers  $x$ .  
 d)  $\lfloor \sqrt{\lceil x \rceil} \rfloor = \lfloor \sqrt{x} \rfloor$  for all positive real numbers  $x$ .  
 e)  $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$  for all real numbers  $x$  and  $y$ .
75. Prove that if  $x$  is a positive real number, then  
 a)  $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$ .  
 b)  $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$ .
76. Let  $x$  be a real number. Show that  $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$ .
77. For each of these partial functions, determine its domain, codomain, domain of definition, and the set of values for which it is undefined. Also, determine whether it is a total function.  
 a)  $f: \mathbf{Z} \rightarrow \mathbf{R}, f(n) = 1/n$   
 b)  $f: \mathbf{Z} \rightarrow \mathbf{Z}, f(n) = \lceil n/2 \rceil$   
 c)  $f: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Q}, f(m, n) = m/n$   
 d)  $f: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}, f(m, n) = mn$   
 e)  $f: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}, f(m, n) = m - n$  if  $m > n$
78. a) Show that a partial function from  $A$  to  $B$  can be viewed as a function  $f^*$  from  $A$  to  $B \cup \{u\}$ , where  $u$  is not an element of  $B$  and
- $$f^*(a) = \begin{cases} f(a) & \text{if } a \text{ belongs to the domain of definition of } f \\ u & \text{if } f \text{ is undefined at } a. \end{cases}$$
- b) Using the construction in (a), find the function  $f^*$  corresponding to each partial function in Exercise 77.
79. a) Show that if a set  $S$  has cardinality  $m$ , where  $m$  is a positive integer, then there is a one-to-one correspondence between  $S$  and the set  $\{1, 2, \dots, m\}$ .  
 b) Show that if  $S$  and  $T$  are two sets each with  $m$  elements, where  $m$  is a positive integer, then there is a one-to-one correspondence between  $S$  and  $T$ .
- \*80. Show that a set  $S$  is infinite if and only if there is a proper subset  $A$  of  $S$  such that there is a one-to-one correspondence between  $A$  and  $S$ .

**SOME INFINITE SERIES** Although most of the summations in this book are finite sums, infinite series are important in some parts of discrete mathematics. Infinite series are usually studied in a course in calculus and even the definition of these series requires the use of calculus, but sometimes they arise in discrete mathematics, because discrete mathematics deals with infinite collections of discrete elements. In particular, in our future studies in discrete mathematics, we will find the closed forms for the infinite series in Examples 24 and 25 to be quite useful.

**EXAMPLE 24** (Requires calculus) Let  $x$  be a real number with  $|x| < 1$ . Find  $\sum_{n=0}^{\infty} x^n$ .



**Solution:** By Theorem 1 with  $a = 1$  and  $r = x$  we see that  $\sum_{n=0}^k x^n = \frac{x^{k+1} - 1}{x - 1}$ . Because  $|x| < 1$ ,  $x^{k+1}$  approaches 0 as  $k$  approaches infinity. It follows that

$$\sum_{n=0}^{\infty} x^n = \lim_{k \rightarrow \infty} \frac{x^{k+1} - 1}{x - 1} = \frac{0 - 1}{x - 1} = \frac{1}{1 - x}.$$

We can produce new summation formulae by differentiating or integrating existing formulae.

**EXAMPLE 25** (Requires calculus) Differentiating both sides of the equation

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1 - x},$$

from Example 24 we find that


$$\sum_{k=1}^{\infty} kx^{k-1} = \frac{1}{(1 - x)^2}.$$


(This differentiation is valid for  $|x| < 1$  by a theorem about infinite series.)

## Exercises

- Find these terms of the sequence  $\{a_n\}$ , where  $a_n = 2 \cdot (-3)^n + 5^n$ .  
a)  $a_0$     b)  $a_1$     c)  $a_4$     d)  $a_5$
- What is the term  $a_8$  of the sequence  $\{a_n\}$  if  $a_n$  equals  
a)  $2^{n-1}$ ?    b)  $7$ ?  
c)  $1 + (-1)^n$ ?    d)  $-(-2)^n$ ?
- What are the terms  $a_0, a_1, a_2$ , and  $a_3$  of the sequence  $\{a_n\}$ , where  $a_n$  equals  
a)  $2^n + 1$ ?    b)  $(n + 1)^{n+1}$ ?  
c)  $\lfloor n/2 \rfloor$ ?    d)  $\lfloor n/2 \rfloor + \lceil n/2 \rceil$ ?
- What are the terms  $a_0, a_1, a_2$ , and  $a_3$  of the sequence  $\{a_n\}$ , where  $a_n$  equals  
a)  $(-2)^n$ ?    b)  $3$ ?  
c)  $7 + 4^n$ ?    d)  $2^n + (-2)^n$ ?
- List the first 10 terms of each of these sequences.  
a) the sequence that begins with 2 and in which each successive term is 3 more than the preceding term  
b) the sequence that lists each positive integer three times, in increasing order  
c) the sequence that lists the odd positive integers in increasing order, listing each odd integer twice  
d) the sequence whose  $n$ th term is  $n! - 2^n$   
e) the sequence that begins with 3, where each succeeding term is twice the preceding term  
f) the sequence whose first term is 2, second term is 4, and each succeeding term is the sum of the two preceding terms  
g) the sequence whose  $n$ th term is the number of bits in the binary expansion of the number  $n$  (defined in Section 4.2)  
h) the sequence where the  $n$ th term is the number of letters in the English word for the index  $n$
- List the first 10 terms of each of these sequences.  
a) the sequence obtained by starting with 10 and obtaining each term by subtracting 3 from the previous term  
b) the sequence whose  $n$ th term is the sum of the first  $n$  positive integers  
c) the sequence whose  $n$ th term is  $3^n - 2^n$   
d) the sequence whose  $n$ th term is  $\lfloor \sqrt{n} \rfloor$   
e) the sequence whose first two terms are 1 and 5 and each succeeding term is the sum of the two previous terms



- f) the sequence whose  $n$ th term is the largest integer whose binary expansion (defined in Section 4.2) has  $n$  bits (Write your answer in decimal notation.)
- g) the sequence whose terms are constructed sequentially as follows: start with 1, then add 1, then multiply by 1, then add 2, then multiply by 2, and so on
- h) the sequence whose  $n$ th term is the largest integer  $k$  such that  $k! \leq n$
7. Find at least three different sequences beginning with the terms 1, 2, 4 whose terms are generated by a simple formula or rule.
8. Find at least three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule.
9. Find the first five terms of the sequence defined by each of these recurrence relations and initial conditions.
- $a_n = 6a_{n-1}, a_0 = 2$
  - $a_n = a_{n-1}^2, a_1 = 2$
  - $a_n = a_{n-1} + 3a_{n-2}, a_0 = 1, a_1 = 2$
  - $a_n = na_{n-1} + n^2a_{n-2}, a_0 = 1, a_1 = 1$
  - $a_n = a_{n-1} + a_{n-3}, a_0 = 1, a_1 = 2, a_2 = 0$
10. Find the first six terms of the sequence defined by each of these recurrence relations and initial conditions.
- $a_n = -2a_{n-1}, a_0 = -1$
  - $a_n = a_{n-1} - a_{n-2}, a_0 = 2, a_1 = -1$
  - $a_n = 3a_{n-1}^2, a_0 = 1$
  - $a_n = na_{n-1} + a_{n-2}^2, a_0 = -1, a_1 = 0$
  - $a_n = a_{n-1} - a_{n-2} + a_{n-3}, a_0 = 1, a_1 = 1, a_2 = 2$
11. Let  $a_n = 2^n + 5 \cdot 3^n$  for  $n = 0, 1, 2, \dots$ .
- Find  $a_0, a_1, a_2, a_3$ , and  $a_4$ .
  - Show that  $a_2 = 5a_1 - 6a_0, a_3 = 5a_2 - 6a_1$ , and  $a_4 = 5a_3 - 6a_2$ .
  - Show that  $a_n = 5a_{n-1} - 6a_{n-2}$  for all integers  $n$  with  $n \geq 2$ .
12. Show that the sequence  $\{a_n\}$  is a solution of the recurrence relation  $a_n = -3a_{n-1} + 4a_{n-2}$  if
- $a_n = 0$ .
  - $a_n = 1$ .
  - $a_n = (-4)^n$ .
  - $a_n = 2(-4)^n + 3$ .
13. Is the sequence  $\{a_n\}$  a solution of the recurrence relation  $a_n = 8a_{n-1} - 16a_{n-2}$  if
- $a_n = 0$ ?
  - $a_n = 1$ ?
  - $a_n = 2^n$ ?
  - $a_n = 4^n$ ?
  - $a_n = n4^n$ ?
  - $a_n = 2 \cdot 4^n + 3n4^n$ ?
  - $a_n = (-4)^n$ ?
  - $a_n = n^24^n$ ?
14. For each of these sequences find a recurrence relation satisfied by this sequence. (The answers are not unique because there are infinitely many different recurrence relations satisfied by any sequence.)
- $a_n = 3$
  - $a_n = 2n$
  - $a_n = 2n + 3$
  - $a_n = 5^n$
  - $a_n = n^2$
  - $a_n = n^2 + n$
  - $a_n = n + (-1)^n$
  - $a_n = n!$
15. Show that the sequence  $\{a_n\}$  is a solution of the recurrence relation  $a_n = a_{n-1} + 2a_{n-2} + 2n - 9$  if
- $a_n = -n + 2$ .
  - $a_n = 5(-1)^n - n + 2$ .
  - $a_n = 3(-1)^n + 2^n - n + 2$ .
  - $a_n = 7 \cdot 2^n - n + 2$ .
16. Find the solution to each of these recurrence relations with the given initial conditions. Use an iterative approach such as that used in Example 10.
- $a_n = -a_{n-1}, a_0 = 5$
  - $a_n = a_{n-1} + 3, a_0 = 1$
  - $a_n = a_{n-1} - n, a_0 = 4$
  - $a_n = 2a_{n-1} - 3, a_0 = -1$
  - $a_n = (n + 1)a_{n-1}, a_0 = 2$
  - $a_n = 2na_{n-1}, a_0 = 3$
  - $a_n = -a_{n-1} + n - 1, a_0 = 7$
17. Find the solution to each of these recurrence relations and initial conditions. Use an iterative approach such as that used in Example 10.
- $a_n = 3a_{n-1}, a_0 = 2$
  - $a_n = a_{n-1} + 2, a_0 = 3$
  - $a_n = a_{n-1} + n, a_0 = 1$
  - $a_n = a_{n-1} + 2n + 3, a_0 = 4$
  - $a_n = 2a_{n-1} - 1, a_0 = 1$
  - $a_n = 3a_{n-1} + 1, a_0 = 1$
  - $a_n = na_{n-1}, a_0 = 5$
  - $a_n = 2na_{n-1}, a_0 = 1$
18. A person deposits \$1000 in an account that yields 9% interest compounded annually.
- Set up a recurrence relation for the amount in the account at the end of  $n$  years.
  - Find an explicit formula for the amount in the account at the end of  $n$  years.
  - How much money will the account contain after 100 years?
19. Suppose that the number of bacteria in a colony triples every hour.
- Set up a recurrence relation for the number of bacteria after  $n$  hours have elapsed.
  - If 100 bacteria are used to begin a new colony, how many bacteria will be in the colony in 10 hours?
20. Assume that the population of the world in 2010 was 6.9 billion and is growing at the rate of 1.1% a year.
- 
  - Set up a recurrence relation for the population of the world  $n$  years after 2010.
  - Find an explicit formula for the population of the world  $n$  years after 2010.
  - What will the population of the world be in 2030?
21. A factory makes custom sports cars at an increasing rate. In the first month only one car is made, in the second month two cars are made, and so on, with  $n$  cars made in the  $n$ th month.
- Set up a recurrence relation for the number of cars produced in the first  $n$  months by this factory.
  - How many cars are produced in the first year?
  - Find an explicit formula for the number of cars produced in the first  $n$  months by this factory.
22. An employee joined a company in 2009 with a starting salary of \$50,000. Every year this employee receives a raise of \$1000 plus 5% of the salary of the previous year.

- a) Set up a recurrence relation for the salary of this employee  $n$  years after 2009.
- b) What will the salary of this employee be in 2017?
- c) Find an explicit formula for the salary of this employee  $n$  years after 2009.
23. Find a recurrence relation for the balance  $B(k)$  owed at the end of  $k$  months on a loan of \$5000 at a rate of 7% if a payment of \$100 is made each month. [Hint: Express  $B(k)$  in terms of  $B(k-1)$ ; the monthly interest is  $(0.07/12)B(k-1)$ .]
24.  a) Find a recurrence relation for the balance  $B(k)$  owed at the end of  $k$  months on a loan at a rate of  $r$  if a payment  $P$  is made on the loan each month. [Hint: Express  $B(k)$  in terms of  $B(k-1)$  and note that the monthly interest rate is  $r/12$ .]
- b) Determine what the monthly payment  $P$  should be so that the loan is paid off after  $T$  months.
25. For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list. Assuming that your formula or rule is correct, determine the next three terms of the sequence.
- a) 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, ...
- b) 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, ...
- c) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, ...
- d) 3, 6, 12, 24, 48, 96, 192, ...
- e) 15, 8, 1, -6, -13, -20, -27, ...
- f) 3, 5, 8, 12, 17, 23, 30, 38, 47, ...
- g) 2, 16, 54, 128, 250, 432, 686, ...
- h) 2, 3, 7, 25, 121, 721, 5041, 40321, ...
26. For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list. Assuming that your formula or rule is correct, determine the next three terms of the sequence.
- a) 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, ...
- b) 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, ...
- c) 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, ...
- d) 1, 2, 2, 2, 3, 3, 3, 3, 3, 5, 5, 5, 5, 5, ...
- e) 0, 2, 8, 26, 80, 242, 728, 2186, 6560, 19682, ...
- f) 1, 3, 15, 105, 945, 10395, 135135, 2027025, 34459425, ...
- g) 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, ...
- h) 2, 4, 16, 256, 65536, 4294967296, ...
- \*\*27. Show that if  $a_n$  denotes the  $n$ th positive integer that is not a perfect square, then  $a_n = n + \{\sqrt{n}\}$ , where  $\{x\}$  denotes the integer closest to the real number  $x$ .
- \*28. Let  $a_n$  be the  $n$ th term of the sequence 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, ..., constructed by including the integer  $k$  exactly  $k$  times. Show that  $a_n = \lfloor \sqrt{2n} + \frac{1}{2} \rfloor$ .
29. What are the values of these sums?
- a)  $\sum_{k=1}^5 (k+1)$
- b)  $\sum_{j=0}^4 (-2)^j$
- c)  $\sum_{i=1}^{10} 3$
- d)  $\sum_{j=0}^8 (2^{j+1} - 2^j)$
30. What are the values of these sums, where  $S = \{1, 3, 5, 7\}$ ?
- a)  $\sum_{j \in S} j$
- b)  $\sum_{j \in S} j^2$
- c)  $\sum_{j \in S} (1/j)$
- d)  $\sum_{j \in S} 1$
31. What is the value of each of these sums of terms of a geometric progression?
- a)  $\sum_{j=0}^8 3 \cdot 2^j$
- b)  $\sum_{j=1}^8 2^j$
- c)  $\sum_{j=2}^8 (-3)^j$
- d)  $\sum_{j=0}^8 2 \cdot (-3)^j$
32. Find the value of each of these sums.
- a)  $\sum_{j=0}^8 (1 + (-1)^j)$
- b)  $\sum_{j=0}^8 (3^j - 2^j)$
- c)  $\sum_{j=0}^8 (2 \cdot 3^j + 3 \cdot 2^j)$
- d)  $\sum_{j=0}^8 (2^{j+1} - 2^j)$
33. Compute each of these double sums.
- a)  $\sum_{i=1}^2 \sum_{j=1}^3 (i+j)$
- b)  $\sum_{i=0}^2 \sum_{j=0}^3 (2i+3j)$
- c)  $\sum_{i=1}^3 \sum_{j=0}^2 i$
- d)  $\sum_{i=0}^2 \sum_{j=1}^3 ij$
34. Compute each of these double sums.
- a)  $\sum_{i=1}^3 \sum_{j=1}^2 (i-j)$
- b)  $\sum_{i=0}^3 \sum_{j=0}^2 (3i+2j)$
- c)  $\sum_{i=1}^3 \sum_{j=0}^2 j$
- d)  $\sum_{i=0}^2 \sum_{j=0}^3 i^2 j^3$
35. Show that  $\sum_{j=1}^n (a_j - a_{j-1}) = a_n - a_0$ , where  $a_0, a_1, \dots, a_n$  is a sequence of real numbers. This type of sum is called **telescoping**.
36. Use the identity  $1/(k(k+1)) = 1/k - 1/(k+1)$  and Exercise 35 to compute  $\sum_{k=1}^n 1/(k(k+1))$ .
37. Sum both sides of the identity  $k^2 - (k-1)^2 = 2k - 1$  from  $k = 1$  to  $k = n$  and use Exercise 35 to find
- a) a formula for  $\sum_{k=1}^n (2k - 1)$  (the sum of the first  $n$  odd natural numbers).
- b) a formula for  $\sum_{k=1}^n k$ .
- \*38. Use the technique given in Exercise 35, together with the result of Exercise 37b, to derive the formula for  $\sum_{k=1}^n k^2$  given in Table 2. [Hint: Take  $a_k = k^3$  in the telescoping sum in Exercise 35.]
39. Find  $\sum_{k=100}^{200} k$ . (Use Table 2.)
40. Find  $\sum_{k=99}^{200} k^3$ . (Use Table 2.)
- \*41. Find a formula for  $\sum_{k=0}^m \lfloor \sqrt{k} \rfloor$ , when  $m$  is a positive integer.
- \*42. Find a formula for  $\sum_{k=0}^m \lfloor \sqrt[3]{k} \rfloor$ , when  $m$  is a positive integer.
- There is also a special notation for products. The product of  $a_m, a_{m+1}, \dots, a_n$  is represented by  $\prod_{j=m}^n a_j$ , read as the product from  $j = m$  to  $j = n$  of  $a_j$ .



**Remark:** Because  $\mathbf{Z}_m$  with the operations of addition and multiplication modulo  $m$  satisfies the properties listed,  $\mathbf{Z}_m$  with modular addition is said to be a **commutative group** and  $\mathbf{Z}_m$  with both of these operations is said to be a **commutative ring**. Note that the set of integers with ordinary addition and multiplication also forms a commutative ring. Groups and rings are studied in courses that cover abstract algebra.

**Remark:** In Exercise 30, and in later sections, we will use the notations  $+$  and  $\cdot$  for  $+_m$  and  $\cdot_m$  without the subscript  $m$  on the symbol for the operator whenever we work with  $\mathbf{Z}_m$ .

## Exercises

- Does 17 divide each of these numbers?  
a) 68    b) 84    c) 357    d) 1001
- Prove that if  $a$  is an integer other than 0, then  
a) 1 divides  $a$ .    b)  $a$  divides 0.
- Prove that part (ii) of Theorem 1 is true.
- Prove that part (iii) of Theorem 1 is true.
- Show that if  $a \mid b$  and  $b \mid a$ , where  $a$  and  $b$  are integers, then  $a = b$  or  $a = -b$ .
- Show that if  $a, b, c$ , and  $d$  are integers, where  $a \neq 0$ , such that  $a \mid c$  and  $b \mid d$ , then  $ab \mid cd$ .
- Show that if  $a, b$ , and  $c$  are integers, where  $a \neq 0$  and  $c \neq 0$ , such that  $ac \mid bc$ , then  $a \mid b$ .
- Prove or disprove that if  $a \mid bc$ , where  $a, b$ , and  $c$  are positive integers and  $a \neq 0$ , then  $a \mid b$  or  $a \mid c$ .
- What are the quotient and remainder when  
a) 19 is divided by 7?  
b)  $-111$  is divided by 11?  
c) 789 is divided by 23?  
d) 1001 is divided by 13?  
e) 0 is divided by 19?  
f) 3 is divided by 5?  
g)  $-1$  is divided by 3?  
h) 4 is divided by 1?
- What are the quotient and remainder when  
a) 44 is divided by 8?  
b) 777 is divided by 21?  
c)  $-123$  is divided by 19?  
d)  $-1$  is divided by 23?  
e)  $-2002$  is divided by 87?  
f) 0 is divided by 17?  
g) 1,234,567 is divided by 1001?  
h)  $-100$  is divided by 101?
- What time does a 12-hour clock read  
a) 80 hours after it reads 11:00?  
b) 40 hours before it reads 12:00?  
c) 100 hours after it reads 6:00?
- What time does a 24-hour clock read  
a) 100 hours after it reads 2:00?  
b) 45 hours before it reads 12:00?  
c) 168 hours after it reads 19:00?
- Suppose that  $a$  and  $b$  are integers,  $a \equiv 4 \pmod{13}$ , and  $b \equiv 9 \pmod{13}$ . Find the integer  $c$  with  $0 \leq c \leq 12$  such that  
a)  $c \equiv 9a \pmod{13}$ .  
b)  $c \equiv 11b \pmod{13}$ .  
c)  $c \equiv a + b \pmod{13}$ .  
d)  $c \equiv 2a + 3b \pmod{13}$ .  
e)  $c \equiv a^2 + b^2 \pmod{13}$ .  
f)  $c \equiv a^3 - b^3 \pmod{13}$ .
- Suppose that  $a$  and  $b$  are integers,  $a \equiv 11 \pmod{19}$ , and  $b \equiv 3 \pmod{19}$ . Find the integer  $c$  with  $0 \leq c \leq 18$  such that  
a)  $c \equiv 13a \pmod{19}$ .  
b)  $c \equiv 8b \pmod{19}$ .  
c)  $c \equiv a - b \pmod{19}$ .  
d)  $c \equiv 7a + 3b \pmod{19}$ .  
e)  $c \equiv 2a^2 + 3b^2 \pmod{19}$ .  
f)  $c \equiv a^3 + 4b^3 \pmod{19}$ .
- Let  $m$  be a positive integer. Show that  $a \equiv b \pmod{m}$  if  $a \bmod m = b \bmod m$ .
- Let  $m$  be a positive integer. Show that  $a \bmod m = b \bmod m$  if  $a \equiv b \pmod{m}$ .
- Show that if  $n$  and  $k$  are positive integers, then  $\lceil n/k \rceil = \lfloor (n-1)/k \rfloor + 1$ .
- Show that if  $a$  is an integer and  $d$  is an integer greater than 1, then the quotient and remainder obtained when  $a$  is divided by  $d$  are  $\lfloor a/d \rfloor$  and  $a - d\lfloor a/d \rfloor$ , respectively.
- Find a formula for the integer with smallest absolute value that is congruent to an integer  $a$  modulo  $m$ , where  $m$  is a positive integer.
- Evaluate these quantities.  
a)  $-17 \bmod 2$     b)  $144 \bmod 7$   
c)  $-101 \bmod 13$     d)  $199 \bmod 19$
- Evaluate these quantities.  
a)  $13 \bmod 3$     b)  $-97 \bmod 11$   
c)  $155 \bmod 19$     d)  $-221 \bmod 23$
- Find  $a \operatorname{div} m$  and  $a \bmod m$  when  
a)  $a = -111, m = 99$ .  
b)  $a = -9999, m = 101$ .  
c)  $a = 10299, m = 999$ .  
d)  $a = 123456, m = 1001$ .

23. Find  $a \text{ div } m$  and  $a \text{ mod } m$  when
- $a = 228, m = 119$ .
  - $a = 9009, m = 223$ .
  - $a = -10101, m = 333$ .
  - $a = -765432, m = 38271$ .
24. Find the integer  $a$  such that
- $a \equiv 43 \pmod{23}$  and  $-22 \leq a \leq 0$ .
  - $a \equiv 17 \pmod{29}$  and  $-14 \leq a \leq 14$ .
  - $a \equiv -11 \pmod{21}$  and  $90 \leq a \leq 110$ .
25. Find the integer  $a$  such that
- $a \equiv -15 \pmod{27}$  and  $-26 \leq a \leq 0$ .
  - $a \equiv 24 \pmod{31}$  and  $-15 \leq a \leq 15$ .
  - $a \equiv 99 \pmod{41}$  and  $100 \leq a \leq 140$ .
26. List five integers that are congruent to 4 modulo 12.
27. List all integers between  $-100$  and  $100$  that are congruent to  $-1$  modulo 25.
28. Decide whether each of these integers is congruent to 3 modulo 7.
- 37
  - 66
  - $-17$
  - $-67$
29. Decide whether each of these integers is congruent to 5 modulo 17.
- 80
  - 103
  - $-29$
  - $-122$
30. Find each of these values.
- $(177 \text{ mod } 31 + 270 \text{ mod } 31) \text{ mod } 31$
  - $(177 \text{ mod } 31 \cdot 270 \text{ mod } 31) \text{ mod } 31$
31. Find each of these values.
- $(-133 \text{ mod } 23 + 261 \text{ mod } 23) \text{ mod } 23$
  - $(457 \text{ mod } 23 \cdot 182 \text{ mod } 23) \text{ mod } 23$
32. Find each of these values.
- $(19^2 \text{ mod } 41) \text{ mod } 9$
  - $(32^3 \text{ mod } 13)^2 \text{ mod } 11$
  - $(7^3 \text{ mod } 23)^2 \text{ mod } 31$
  - $(21^2 \text{ mod } 15)^3 \text{ mod } 22$
33. Find each of these values.
- $(99^2 \text{ mod } 32)^3 \text{ mod } 15$
  - $(3^4 \text{ mod } 17)^2 \text{ mod } 11$
  - $(19^3 \text{ mod } 23)^2 \text{ mod } 31$
  - $(89^3 \text{ mod } 79)^4 \text{ mod } 26$
34. Show that if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , where  $a, b, c, d$ , and  $m$  are integers with  $m \geq 2$ , then  $a - c \equiv b - d \pmod{m}$ .
35. Show that if  $n \mid m$ , where  $n$  and  $m$  are integers greater than 1, and if  $a \equiv b \pmod{m}$ , where  $a$  and  $b$  are integers, then  $a \equiv b \pmod{n}$ .
36. Show that if  $a, b, c$ , and  $m$  are integers such that  $m \geq 2$ ,  $c > 0$ , and  $a \equiv b \pmod{m}$ , then  $ac \equiv bc \pmod{mc}$ .
37. Find counterexamples to each of these statements about congruences.
- If  $ac \equiv bc \pmod{m}$ , where  $a, b, c$ , and  $m$  are integers with  $m \geq 2$ , then  $a \equiv b \pmod{m}$ .
  - If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , where  $a, b, c, d$ , and  $m$  are integers with  $c$  and  $d$  positive and  $m \geq 2$ , then  $a^c \equiv b^d \pmod{m}$ .
38. Show that if  $n$  is an integer then  $n^2 \equiv 0$  or  $1 \pmod{4}$ .
39. Use Exercise 38 to show that if  $m$  is a positive integer of the form  $4k + 3$  for some nonnegative integer  $k$ , then  $m$  is not the sum of the squares of two integers.
40. Prove that if  $n$  is an odd positive integer, then  $n^2 \equiv 1 \pmod{8}$ .
41. Show that if  $a, b, k$ , and  $m$  are integers such that  $k \geq 1$ ,  $m \geq 2$ , and  $a \equiv b \pmod{m}$ , then  $a^k \equiv b^k \pmod{m}$ .
42. Show that  $\mathbf{Z}_m$  with addition modulo  $m$ , where  $m \geq 2$  is an integer, satisfies the closure, associative, and commutative properties, 0 is an additive identity, and for every nonzero  $a \in \mathbf{Z}_m$ ,  $m - a$  is an inverse of  $a$  modulo  $m$ .
43. Show that  $\mathbf{Z}_m$  with multiplication modulo  $m$ , where  $m \geq 2$  is an integer, satisfies the closure, associative, and commutativity properties, and 1 is a multiplicative identity.
44. Show that the distributive property of multiplication over addition holds for  $\mathbf{Z}_m$ , where  $m \geq 2$  is an integer.
45. Write out the addition and multiplication tables for  $\mathbf{Z}_5$  (where by addition and multiplication we mean  $+$ <sub>5</sub> and  $\cdot$ <sub>5</sub>).
46. Write out the addition and multiplication tables for  $\mathbf{Z}_6$  (where by addition and multiplication we mean  $+$ <sub>6</sub> and  $\cdot$ <sub>6</sub>).
47. Determine whether each of the functions  $f(a) = a \text{ div } d$  and  $g(a) = a \text{ mod } d$ , where  $d$  is a fixed positive integer, from the set of integers to the set of integers, is one-to-one, and determine whether each of these functions is onto.

## 4.2 Integer Representations and Algorithms

### Introduction

Integers can be expressed using any integer greater than one as a base, as we will show in this section. Although we commonly use decimal (base 10), representations, binary (base 2), octal (base 8), and hexadecimal (base 16) representations are often used, especially in computer science. Given a base  $b$  and an integer  $n$ , we will show how to construct the base  $b$  representation of this integer. We will also explain how to quickly convert between binary and octal and between binary and hexadecimal notations.

Although we cannot divide both sides of a congruence by any integer to produce a valid congruence, we can if this integer is relatively prime to the modulus. Theorem 7 establishes this important fact. We use Lemma 2 in the proof.


**THEOREM 7**

Let  $m$  be a positive integer and let  $a$ ,  $b$ , and  $c$  be integers. If  $ac \equiv bc \pmod{m}$  and  $\gcd(c, m) = 1$ , then  $a \equiv b \pmod{m}$ .

**Proof:** Because  $ac \equiv bc \pmod{m}$ ,  $m \mid ac - bc = c(a - b)$ . By Lemma 2, because  $\gcd(c, m) = 1$ , it follows that  $m \mid a - b$ . We conclude that  $a \equiv b \pmod{m}$ .  $\triangleleft$

## Exercises

- Determine whether each of these integers is prime.
    - 21
    - 29
    - 71
    - 97
    - 111
    - 143
  - Determine whether each of these integers is prime.
    - 19
    - 27
    - 93
    - 101
    - 107
    - 113
  - Find the prime factorization of each of these integers.
    - 88
    - 126
    - 729
    - 1001
    - 1111
    - 909,090
  - Find the prime factorization of each of these integers.
    - 39
    - 81
    - 101
    - 143
    - 289
    - 899
  - Find the prime factorization of  $10!$ .
  - \* How many zeros are there at the end of  $100!$ ?
  - Express in pseudocode the trial division algorithm for determining whether an integer is prime.
  - Express in pseudocode the algorithm described in the text for finding the prime factorization of an integer.
  - Show that if  $a^m + 1$  is composite if  $a$  and  $m$  are integers greater than 1 and  $m$  is odd. [Hint: Show that  $x + 1$  is a factor of the polynomial  $x^m + 1$  if  $m$  is odd.]
  - Show that if  $2^m + 1$  is an odd prime, then  $m = 2^n$  for some nonnegative integer  $n$ . [Hint: First show that the polynomial identity  $x^m + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + \dots - x^k + 1)$  holds, where  $m = kt$  and  $t$  is odd.]
  - \* Show that  $\log_2 3$  is an irrational number. Recall that an irrational number is a real number  $x$  that cannot be written as the ratio of two integers.
  - Prove that for every positive integer  $n$ , there are  $n$  consecutive composite integers. [Hint: Consider the  $n$  consecutive integers starting with  $(n + 1)! + 2$ .]
  - \* Prove or disprove that there are three consecutive odd positive integers that are primes, that is, odd primes of the form  $p$ ,  $p + 2$ , and  $p + 4$ .
  - Which positive integers less than 12 are relatively prime to 12?
  - Which positive integers less than 30 are relatively prime to 30?
  - Determine whether the integers in each of these sets are pairwise relatively prime.
    - 21, 34, 55
    - 14, 17, 85
    - 25, 41, 49, 64
    - 17, 18, 19, 23
  - Determine whether the integers in each of these sets are pairwise relatively prime.
    - 11, 15, 19
    - 14, 15, 21
    - 12, 17, 31, 37
    - 7, 8, 9, 11
  - We call a positive integer **perfect** if it equals the sum of its positive divisors other than itself.
    - Show that 6 and 28 are perfect.
    - Show that  $2^{p-1}(2^p - 1)$  is a perfect number when  $2^p - 1$  is prime.
  - Show that if  $2^n - 1$  is prime, then  $n$  is prime. [Hint: Use the identity  $2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)$ .]
  - Determine whether each of these integers is prime, verifying some of Mersenne's claims.
    - $2^7 - 1$
    - $2^9 - 1$
    - $2^{11} - 1$
    - $2^{13} - 1$
- The value of the **Euler  $\phi$ -function** at the positive integer  $n$  is defined to be the number of positive integers less than or equal to  $n$  that are relatively prime to  $n$ . [Note:  $\phi$  is the Greek letter phi.]
- Find these values of the Euler  $\phi$ -function.
    - $\phi(4)$ .
    - $\phi(10)$ .
    - $\phi(13)$ .
  - Show that  $n$  is prime if and only if  $\phi(n) = n - 1$ .
  - What is the value of  $\phi(p^k)$  when  $p$  is prime and  $k$  is a positive integer?
  - What are the greatest common divisors of these pairs of integers?
    - $2^2 \cdot 3^3 \cdot 5^5, 2^5 \cdot 3^3 \cdot 5^2$
    - $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

- c)  $17, 17^{17}$       d)  $2^2 \cdot 7, 5^3 \cdot 13$   
 e) 0, 5      f)  $2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7$
25. What are the greatest common divisors of these pairs of integers?  
 a)  $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$   
 b)  $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$   
 c)  $23^{31}, 23^{17}$   
 d)  $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$   
 e)  $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$   
 f) 1111, 0
26. What is the least common multiple of each pair in Exercise 24?
27. What is the least common multiple of each pair in Exercise 25?
28. Find  $\gcd(1000, 625)$  and  $\text{lcm}(1000, 625)$  and verify that  $\gcd(1000, 625) \cdot \text{lcm}(1000, 625) = 1000 \cdot 625$ .
29. Find  $\gcd(92928, 123552)$  and  $\text{lcm}(92928, 123552)$ , and verify that  $\gcd(92928, 123552) \cdot \text{lcm}(92928, 123552) = 92928 \cdot 123552$ . [Hint: First find the prime factorizations of 92928 and 123552.]
30. If the product of two integers is  $2^7 3^8 5^2 7^{11}$  and their greatest common divisor is  $2^3 3^4 5$ , what is their least common multiple?
31. Show that if  $a$  and  $b$  are positive integers, then  $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$ . [Hint: Use the prime factorizations of  $a$  and  $b$  and the formulae for  $\gcd(a, b)$  and  $\text{lcm}(a, b)$  in terms of these factorizations.]
32. Use the Euclidean algorithm to find  
 a)  $\gcd(1, 5)$ .      b)  $\gcd(100, 101)$ .  
 c)  $\gcd(123, 277)$ .      d)  $\gcd(1529, 14039)$ .  
 e)  $\gcd(1529, 14038)$ .      f)  $\gcd(11111, 111111)$ .
33. Use the Euclidean algorithm to find  
 a)  $\gcd(12, 18)$ .      b)  $\gcd(111, 201)$ .  
 c)  $\gcd(1001, 1331)$ .      d)  $\gcd(12345, 54321)$ .  
 e)  $\gcd(1000, 5040)$ .      f)  $\gcd(9888, 6060)$ .
34. How many divisions are required to find  $\gcd(21, 34)$  using the Euclidean algorithm?
35. How many divisions are required to find  $\gcd(34, 55)$  using the Euclidean algorithm?
- \*36. Show that if  $a$  and  $b$  are both positive integers, then  $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$ .
-  \*37. Use Exercise 36 to show that if  $a$  and  $b$  are positive integers, then  $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$ . [Hint: Show that the remainders obtained when the Euclidean algorithm is used to compute  $\gcd(2^a - 1, 2^b - 1)$  are of the form  $2^r - 1$ , where  $r$  is a remainder arising when the Euclidean algorithm is used to find  $\gcd(a, b)$ .]
38. Use Exercise 37 to show that the integers  $2^{35} - 1, 2^{34} - 1, 2^{33} - 1, 2^{31} - 1, 2^{29} - 1$ , and  $2^{23} - 1$  are pairwise relatively prime.
39. Using the method followed in Example 17, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.  
 a) 10, 11      b) 21, 44      c) 36, 48  
 d) 34, 55      e) 117, 213      f) 0, 223  
 g) 123, 2347      h) 3454, 4666      i) 9999, 11111

40. Using the method followed in Example 17, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

- a) 9, 11      b) 33, 44      c) 35, 78  
 d) 21, 55      e) 101, 203      f) 124, 323  
 g) 2002, 2339      h) 3457, 4669      i) 10001, 13422

The **extended Euclidean algorithm** can be used to express  $\gcd(a, b)$  as a linear combination with integer coefficients of the integers  $a$  and  $b$ . We set  $s_0 = 1, s_1 = 0, t_0 = 0$ , and  $t_1 = 1$  and let  $s_j = s_{j-2} - q_{j-1}s_{j-1}$  and  $t_j = t_{j-2} - q_{j-1}t_{j-1}$  for  $j = 2, 3, \dots, n$ , where the  $q_j$  are the quotients in the divisions used when the Euclidean algorithm finds  $\gcd(a, b)$ , as shown in the text. It can be shown (see [Ro10]) that  $\gcd(a, b) = s_n a + t_n b$ . The main advantage of the extended Euclidean algorithm is that it uses one pass through the steps of the Euclidean algorithm to find Bézout coefficients of  $a$  and  $b$ , unlike the method in the text which uses two passes.

41. Use the extended Euclidean algorithm to express  $\gcd(26, 91)$  as a linear combination of 26 and 91.
42. Use the extended Euclidean algorithm to express  $\gcd(252, 356)$  as a linear combination of 252 and 356.
43. Use the extended Euclidean algorithm to express  $\gcd(144, 89)$  as a linear combination of 144 and 89.
44. Use the extended Euclidean algorithm to express  $\gcd(1001, 100001)$  as a linear combination of 1001 and 100001.
45. Describe the extended Euclidean algorithm using pseudocode.
46. Find the smallest positive integer with exactly  $n$  different positive factors when  $n$  is  
 a) 3.      b) 4.      c) 5.  
 d) 6.      e) 10.
47. Can you find a formula or rule for the  $n$ th term of a sequence related to the prime numbers or prime factorizations so that the initial terms of the sequence have these values?  
 a) 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, ...  
 b) 1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, ...  
 c) 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, ...  
 d) 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, ...  
 e) 1, 2, 3, 3, 5, 5, 7, 7, 7, 11, 11, 13, 13, ...  
 f) 1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, ...
48. Can you find a formula or rule for the  $n$ th term of a sequence related to the prime numbers or prime factorizations so that the initial terms of the sequence have these values?  
 a) 2, 2, 3, 5, 5, 7, 7, 11, 11, 11, 11, 13, 13, ...  
 b) 0, 1, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 6, 6, ...  
 c) 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, ...  
 d) 1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, ...  
 e) 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, ...  
 f) 4, 9, 25, 49, 121, 169, 289, 361, 529, 841, 961, 1369, ...
49. Prove that the product of any three consecutive integers is divisible by 6.

50. Show that if  $a, b$ , and  $m$  are integers such that  $m \geq 2$  and  $a \equiv b \pmod{m}$ , then  $\gcd(a, m) = \gcd(b, m)$ .
- \*51. Prove or disprove that  $n^2 - 79n + 1601$  is prime whenever  $n$  is a positive integer.
52. Prove or disprove that  $p_1 p_2 \cdots p_n + 1$  is prime for every positive integer  $n$ , where  $p_1, p_2, \dots, p_n$  are the  $n$  smallest prime numbers.
53. Show that there is a composite integer in every arithmetic progression  $ak + b, k = 1, 2, \dots$  where  $a$  and  $b$  are positive integers.
54. Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form  $3k + 2$ , where  $k$  is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes  $q_1, q_2, \dots, q_n$ , and consider the number  $3q_1 q_2 \cdots q_n - 1$ .]
55. Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form  $4k + 3$ , where  $k$  is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes  $q_1, q_2, \dots, q_n$ , and consider the number  $4q_1 q_2 \cdots q_n - 1$ .]
- \*56. Prove that the set of positive rational numbers is countable by setting up a function that assigns to a rational number  $p/q$  with  $\gcd(p, q) = 1$  the base 11 number formed by the decimal representation of  $p$  followed by the base 11 digit A, which corresponds to the decimal number 10, followed by the decimal representation of  $q$ .
- \*57. Prove that the set of positive rational numbers is countable by showing that the function  $K$  is a one-to-one correspondence between the set of positive rational numbers and the set of positive integers if  $K(m/n) = p_1^{2a_1} p_2^{2a_2} \cdots p_s^{2a_s} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_t^{2b_t-1}$ , where  $\gcd(m, n) = 1$  and the prime-power factorizations of  $m$  and  $n$  are  $m = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$  and  $n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$ .

## 4.4 Solving Congruences

### Introduction

Solving linear congruences, which have the form  $ax \equiv b \pmod{m}$ , is an essential task in the study of number theory and its applications, just as solving linear equations plays an important role in calculus and linear algebra. To solve linear congruences, we employ inverses modulo  $m$ . We explain how to work backwards through the steps of the Euclidean algorithm to find inverses modulo  $m$ . Once we have found an inverse of  $a$  modulo  $m$ , we solve the congruence  $ax \equiv b \pmod{m}$  by multiplying both sides of the congruence by this inverse.

Simultaneous systems of linear congruence have been studied since ancient times. For example, the Chinese mathematician Sun-Tsu studied them in the first century. We will show how to solve systems of linear congruences modulo pairwise relatively prime moduli. The result we will prove is called the Chinese remainder theorem, and our proof will give a method to find all solutions of such systems of congruences. We will also show how to use the Chinese remainder theorem as a basis for performing arithmetic with large integers.


We will introduce a useful result of Fermat, known as Fermat's little theorem, which states that if  $p$  is prime and  $p$  does not divide  $a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ . We will examine the converse of this statement, which will lead us to the concept of a pseudoprime. A pseudoprime  $m$  to the base  $a$  is a composite integer  $m$  that masquerades as a prime by satisfying the congruence  $a^{m-1} \equiv 1 \pmod{m}$ . We will also give an example of a Carmichael number, which is a composite integer that is a pseudoprime to all bases  $a$  relatively prime to it.

We also introduce the notion of discrete logarithms, which are analogous to ordinary logarithms. To define discrete logarithms we must first define primitive roots. A primitive root of a prime  $p$  is an integer  $r$  such that every integer not divisible by  $p$  is congruent to a power of  $r$  modulo  $p$ . If  $r$  is a primitive root of  $p$  and  $r^e \equiv a \pmod{p}$ , then  $e$  is the discrete logarithm of  $a$  modulo  $p$  to the base  $r$ . Finding discrete logarithms turns out to be an extremely difficult problem in general. The difficulty of this problem is the basis for the security of many cryptographic systems.



**EXAMPLE 12** Determine whether 2 and 3 are primitive roots modulo 11.


*Solution:* When we compute the powers of 2 in  $\mathbf{Z}_{11}$ , we obtain  $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$ . Because every element of  $\mathbf{Z}_{11}$  is a power of 2, 2 is a primitive root of 11.

When we compute the powers of 3 modulo 11, we obtain  $3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$ . We note that this pattern repeats when we compute higher powers of 3. Because not all elements of  $\mathbf{Z}_{11}$  are powers of 3, we conclude that 3 is not a primitive root of 11. 

An important fact in number theory is that there is a primitive root modulo  $p$  for every prime  $p$ . We refer the reader to [Ro10] for a proof of this fact. Suppose that  $p$  is prime and  $r$  is a primitive root modulo  $p$ . If  $a$  is an integer between 1 and  $p - 1$ , that is, an element of  $\mathbf{Z}_p$ , we know that there is a unique exponent  $e$  such that  $r^e = a$  in  $\mathbf{Z}_p$ , that is,  $r^e \bmod p = a$ .

**DEFINITION 4** Suppose that  $p$  is a prime,  $r$  is a primitive root modulo  $p$ , and  $a$  is an integer between 1 and  $p - 1$  inclusive. If  $r^e \bmod p = a$  and  $0 \leq e \leq p - 1$ , we say that  $e$  is the *discrete logarithm* of  $a$  modulo  $p$  to the base  $r$  and we write  $\log_r a = e$  (where the prime  $p$  is understood).


**EXAMPLE 13** Find the discrete logarithms of 3 and 5 modulo 11 to the base 2.

*Solution:* When we computed the powers of 2 modulo 11 in Example 12, we found that  $2^8 = 3$  and  $2^4 = 5$  in  $\mathbf{Z}_{11}$ . Hence, the discrete logarithms of 3 and 5 modulo 11 to the base 2 are 8 and 4, respectively. (These are the powers of 2 that equal 3 and 5, respectively, in  $\mathbf{Z}_{11}$ .) We write  $\log_2 3 = 8$  and  $\log_2 5 = 4$  (where the modulus 11 is understood and not explicitly noted in the notation). 


The discrete logarithm problem is hard!

The **discrete logarithm problem** takes as input a prime  $p$ , a primitive root  $r$  modulo  $p$ , and a positive integer  $a \in \mathbf{Z}_p$ ; its output is the discrete logarithm of  $a$  modulo  $p$  to the base  $r$ . Although this problem might seem not to be that difficult, it turns out that no polynomial time algorithm is known for solving it. The difficulty of this problem plays an important role in cryptography, as we will see in Section 4.6

## Exercises

1. Show that 15 is an inverse of 7 modulo 26.
-  2. Show that 937 is an inverse of 13 modulo 2436.
3. By inspection (as discussed prior to Example 1), find an inverse of 4 modulo 9.
4. By inspection (as discussed prior to Example 1), find an inverse of 2 modulo 17.
5. Find an inverse of  $a$  modulo  $m$  for each of these pairs of relatively prime integers using the method followed in Example 2.
  - a)  $a = 4, m = 9$
  - b)  $a = 19, m = 141$
  - c)  $a = 55, m = 89$
  - d)  $a = 89, m = 232$
6. Find an inverse of  $a$  modulo  $m$  for each of these pairs of relatively prime integers using the method followed in Example 2.
  - a)  $a = 2, m = 17$
  - b)  $a = 34, m = 89$
  - c)  $a = 144, m = 233$
  - d)  $a = 200, m = 1001$
- \*7. Show that if  $a$  and  $m$  are relatively prime positive integers, then the inverse of  $a$  modulo  $m$  is unique modulo  $m$ . [Hint: Assume that there are two solutions  $b$  and  $c$  of the congruence  $ax \equiv 1 \pmod{m}$ . Use Theorem 7 of Section 4.3 to show that  $b \equiv c \pmod{m}$ .]
8. Show that an inverse of  $a$  modulo  $m$ , where  $a$  is an integer and  $m > 2$  is a positive integer, does not exist if  $\gcd(a, m) > 1$ .
9. Solve the congruence  $4x \equiv 5 \pmod{9}$  using the inverse of 4 modulo 9 found in part (a) of Exercise 5.
10. Solve the congruence  $2x \equiv 7 \pmod{17}$  using the inverse of 2 modulo 7 found in part (a) of Exercise 6.
11. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 5.
  - a)  $19x \equiv 4 \pmod{141}$
  - b)  $55x \equiv 34 \pmod{89}$
  - c)  $89x \equiv 2 \pmod{232}$

12. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 6.
  - a)  $34x \equiv 77 \pmod{89}$
  - b)  $144x \equiv 4 \pmod{233}$
  - c)  $200x \equiv 13 \pmod{1001}$
13. Find the solutions of the congruence  $15x^2 + 19x \equiv 5 \pmod{11}$ . [Hint: Show the congruence is equivalent to the congruence  $15x^2 + 19x + 6 \equiv 0 \pmod{11}$ . Factor the left-hand side of the congruence; show that a solution of the quadratic congruence is a solution of one of the two different linear congruences.]
14. Find the solutions of the congruence  $12x^2 + 25x \equiv 10 \pmod{11}$ . [Hint: Show the congruence is equivalent to the congruence  $12x^2 + 25x + 12 \equiv 0 \pmod{11}$ . Factor the left-hand side of the congruence; show that a solution of the quadratic congruence is a solution of one of two different linear congruences.]
- \*15. Show that if  $m$  is an integer greater than 1 and  $ac \equiv bc \pmod{m}$ , then  $a \equiv b \pmod{m/\gcd(c, m)}$ .
16. a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.  
b) Use part (a) to show that  $10! \equiv -1 \pmod{11}$ .
17. Show that if  $p$  is prime, the only solutions of  $x^2 \equiv 1 \pmod{p}$  are integers  $x$  such that  $x \equiv 1 \pmod{p}$  or  $x \equiv -1 \pmod{p}$ .
- \*18. a) Generalize the result in part (a) of Exercise 16; that is, show that if  $p$  is a prime, the positive integers less than  $p$ , except 1 and  $p-1$ , can be split into  $(p-3)/2$  pairs of integers such that each pair consists of integers that are inverses of each other. [Hint: Use the result of Exercise 17.]  
b) From part (a) conclude that  $(p-1)! \equiv -1 \pmod{p}$  whenever  $p$  is prime. This result is known as **Wilson's theorem**.  
c) What can we conclude if  $n$  is a positive integer such that  $(n-1)! \not\equiv -1 \pmod{n}$ ?
- \*19. This exercise outlines a proof of Fermat's little theorem.
  - a) Suppose that  $a$  is not divisible by the prime  $p$ . Show that no two of the integers  $1 \cdot a, 2 \cdot a, \dots, (p-1)a$  are congruent modulo  $p$ .
  - b) Conclude from part (a) that the product of  $1, 2, \dots, p-1$  is congruent modulo  $p$  to the product of  $a, 2a, \dots, (p-1)a$ . Use this to show that
 
$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}.$$
  - c) Use Theorem 7 of Section 4.3 to show from part (b) that  $a^{p-1} \equiv 1 \pmod{p}$  if  $p \nmid a$ . [Hint: Use Lemma 3 of Section 4.3 to show that  $p$  does not divide  $(p-1)!$  and then use Theorem 7 of Section 4.3. Alternatively, use Wilson's theorem from Exercise 18(b).]
  - d) Use part (c) to show that  $a^p \equiv a \pmod{p}$  for all integers  $a$ .
20. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences  $x \equiv 2 \pmod{3}$ ,  $x \equiv 1 \pmod{4}$ , and  $x \equiv 3 \pmod{5}$ .
21. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences  $x \equiv 1 \pmod{2}$ ,  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$ , and  $x \equiv 4 \pmod{11}$ .
22. Solve the system of congruence  $x \equiv 3 \pmod{6}$  and  $x \equiv 4 \pmod{7}$  using the method of back substitution.
23. Solve the system of congruences in Exercise 20 using the method of back substitution.
24. Solve the system of congruences in Exercise 21 using the method of back substitution.
25. Write out in pseudocode an algorithm for solving a simultaneous system of linear congruences based on the construction in the proof of the Chinese remainder theorem.
- \*26. Find all solutions, if any, to the system of congruences  $x \equiv 5 \pmod{6}$ ,  $x \equiv 3 \pmod{10}$ , and  $x \equiv 8 \pmod{15}$ .
- \*27. Find all solutions, if any, to the system of congruences  $x \equiv 7 \pmod{9}$ ,  $x \equiv 4 \pmod{12}$ , and  $x \equiv 16 \pmod{21}$ .
28. Use the Chinese remainder theorem to show that an integer  $a$ , with  $0 \leq a < m = m_1 m_2 \cdots m_n$ , where the positive integers  $m_1, m_2, \dots, m_n$  are pairwise relatively prime, can be represented uniquely by the  $n$ -tuple  $(a \bmod m_1, a \bmod m_2, \dots, a \bmod m_n)$ .
- \*29. Let  $m_1, m_2, \dots, m_n$  be pairwise relatively prime integers greater than or equal to 2. Show that if  $a \equiv b \pmod{m_i}$  for  $i = 1, 2, \dots, n$ , then  $a \equiv b \pmod{m}$ , where  $m = m_1 m_2 \cdots m_n$ . (This result will be used in Exercise 30 to prove the Chinese remainder theorem. Consequently, do not use the Chinese remainder theorem to prove it.)
- \*30. Complete the proof of the Chinese remainder theorem by showing that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli is unique modulo the product of these moduli. [Hint: Assume that  $x$  and  $y$  are two simultaneous solutions. Show that  $m_i \mid x - y$  for all  $i$ . Using Exercise 29, conclude that  $m = m_1 m_2 \cdots m_n \mid x - y$ .]
31. Which integers leave a remainder of 1 when divided by 2 and also leave a remainder of 1 when divided by 3?
32. Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?
33. Use Fermat's little theorem to find  $7^{121} \bmod 13$ .
34. Use Fermat's little theorem to find  $23^{1002} \bmod 41$ .
35. Use Fermat's little theorem to show that if  $p$  is prime and  $p \nmid a$ , then  $a^{p-2}$  is an inverse of  $a$  modulo  $p$ .
36. Use Exercise 35 to find an inverse of 5 modulo 41.
37. a) Show that  $2^{340} \equiv 1 \pmod{11}$  by Fermat's little theorem and noting that  $2^{340} = (2^{10})^{34}$ .  
b) Show that  $2^{340} \equiv 1 \pmod{31}$  using the fact that  $2^{340} = (2^5)^{68} = 32^{68}$ .  
c) Conclude from parts (a) and (b) that  $2^{340} \equiv 1 \pmod{341}$ .

38. a) Use Fermat's little theorem to compute  $3^{302} \bmod 5$ ,  $3^{302} \bmod 7$ , and  $3^{302} \bmod 11$ .  
 b) Use your results from part (a) and the Chinese remainder theorem to find  $3^{302} \bmod 385$ . (Note that  $385 = 5 \cdot 7 \cdot 11$ .)
39. a) Use Fermat's little theorem to compute  $5^{2003} \bmod 7$ ,  $5^{2003} \bmod 11$ , and  $5^{2003} \bmod 13$ .  
 b) Use your results from part (a) and the Chinese remainder theorem to find  $5^{2003} \bmod 1001$ . (Note that  $1001 = 7 \cdot 11 \cdot 13$ .)
40. Show with the help of Fermat's little theorem that if  $n$  is a positive integer, then 42 divides  $n^7 - n$ .
41. Show that if  $p$  is an odd prime, then every divisor of the Mersenne number  $2^p - 1$  is of the form  $2kp + 1$ , where  $k$  is a nonnegative integer. [Hint: Use Fermat's little theorem and Exercise 37 of Section 4.3.]
42. Use Exercise 41 to determine whether  $M_{13} = 2^{13} - 1 = 8191$  and  $M_{23} = 2^{23} - 1 = 8,388,607$  are prime.
43. Use Exercise 41 to determine whether  $M_{11} = 2^{11} - 1 = 2047$  and  $M_{17} = 2^{17} - 1 = 131,071$  are prime.
-  Let  $n$  be a positive integer and let  $n - 1 = 2^s t$ , where  $s$  is a nonnegative integer and  $t$  is an odd positive integer. We say that  $n$  passes **Miller's test for the base  $b$**  if either  $b^t \equiv 1 \pmod{n}$  or  $b^{2^j t} \equiv -1 \pmod{n}$  for some  $j$  with  $0 \leq j \leq s - 1$ . It can be shown (see [Ro10]) that a composite integer  $n$  passes Miller's test for fewer than  $n/4$  bases  $b$  with  $1 < b < n$ . A composite positive integer  $n$  that passes Miller's test to the base  $b$  is called a **strong pseudoprime to the base  $b$** .
- \*44. Show that if  $n$  is prime and  $b$  is a positive integer with  $n \nmid b$ , then  $n$  passes Miller's test to the base  $b$ .
45. Show that 2047 is a strong pseudoprime to the base 2 by showing that it passes Miller's test to the base 2, but is composite.
46. Show that 1729 is a Carmichael number.
47. Show that 2821 is a Carmichael number.
- \*48. Show that if  $n = p_1 p_2 \cdots p_k$ , where  $p_1, p_2, \dots, p_k$  are distinct primes that satisfy  $p_j - 1 \mid n - 1$  for  $j = 1, 2, \dots, k$ , then  $n$  is a Carmichael number.
49. a) Use Exercise 48 to show that every integer of the form  $(6m + 1)(12m + 1)(18m + 1)$ , where  $m$  is a positive integer and  $6m + 1$ ,  $12m + 1$ , and  $18m + 1$  are all primes, is a Carmichael number.  
 b) Use part (a) to show that 172,947,529 is a Carmichael number.
50. Find the nonnegative integer  $a$  less than 28 represented by each of these pairs, where each pair represents  $(a \bmod 4, a \bmod 7)$ .
- |           |           |           |
|-----------|-----------|-----------|
| a) (0, 0) | b) (1, 0) | c) (1, 1) |
| d) (2, 1) | e) (2, 2) | f) (0, 3) |
| g) (2, 0) | h) (3, 5) | i) (3, 6) |
51. Express each nonnegative integer  $a$  less than 15 as a pair  $(a \bmod 3, a \bmod 5)$ .
52. Explain how to use the pairs found in Exercise 51 to add 4 and 7.
53. Solve the system of congruences that arises in Example 8.
54. Show that 2 is a primitive root of 19.
55. Find the discrete logarithms of 5 and 6 to the base 2 modulo 19.
56. Let  $p$  be an odd prime and  $r$  a primitive root of  $p$ . Show that if  $a$  and  $b$  are positive integers in  $\mathbf{Z}_p$ , then  $\log_r(ab) \equiv \log_r a + \log_r b \pmod{p-1}$ .
57. Write out a table of discrete logarithms modulo 17 with respect to the primitive root 3.
- If  $m$  is a positive integer, the integer  $a$  is a **quadratic residue** of  $m$  if  $\gcd(a, m) = 1$  and the congruence  $x^2 \equiv a \pmod{m}$  has a solution. In other words, a quadratic residue of  $m$  is an integer relatively prime to  $m$  that is a perfect square modulo  $m$ . If  $a$  is not a quadratic residue of  $m$  and  $\gcd(a, m) = 1$ , we say that it is a **quadratic nonresidue** of  $m$ . For example, 2 is a quadratic residue of 7 because  $\gcd(2, 7) = 1$  and  $3^2 \equiv 2 \pmod{7}$  and 3 is a quadratic nonresidue of 7 because  $\gcd(3, 7) = 1$  and  $x^2 \equiv 3 \pmod{7}$  has no solution.
58. Which integers are quadratic residues of 11?
59. Show that if  $p$  is an odd prime and  $a$  is an integer not divisible by  $p$ , then the congruence  $x^2 \equiv a \pmod{p}$  has either no solutions or exactly two incongruent solutions modulo  $p$ .
60. Show that if  $p$  is an odd prime, then there are exactly  $(p-1)/2$  quadratic residues of  $p$  among the integers  $1, 2, \dots, p-1$ .
- If  $p$  is an odd prime and  $a$  is an integer not divisible by  $p$ , the **Legendre symbol**  $\left(\frac{a}{p}\right)$  is defined to be 1 if  $a$  is a quadratic residue of  $p$  and  $-1$  otherwise.
61. Show that if  $p$  is an odd prime and  $a$  and  $b$  are integers with  $a \equiv b \pmod{p}$ , then
- $$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$
62. Prove **Euler's criterion**, which states that if  $p$  is an odd prime and  $a$  is a positive integer not divisible by  $p$ , then
- $$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$
- [Hint: If  $a$  is a quadratic residue modulo  $p$ , apply Fermat's little theorem; otherwise, apply Wilson's theorem, given in Exercise 18(b).]
63. Use Exercise 62 to show that if  $p$  is an odd prime and  $a$  and  $b$  are integers not divisible by  $p$ , then
- $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$
64. Show that if  $p$  is an odd prime, then  $-1$  is a quadratic residue of  $p$  if  $p \equiv 1 \pmod{4}$ , and  $-1$  is not a quadratic residue of  $p$  if  $p \equiv 3 \pmod{4}$ . [Hint: Use Exercise 62.]
65. Find all solutions of the congruence  $x^2 \equiv 29 \pmod{35}$ . [Hint: Find the solutions of this congruence modulo 5 and modulo 7, and then use the Chinese remainder theorem.]



66. Find all solutions of the congruence  $x^2 \equiv 16 \pmod{105}$ .  
 [Hint: Find the solutions of this congruence modulo 3, modulo 5, and modulo 7, and then use the Chinese remainder theorem.]
67. Describe a brute force algorithm for solving the discrete logarithm problem and find the worst-case and average-case time complexity of this algorithm.

## 4.5 Applications of Congruences

Congruences have many applications to discrete mathematics, computer science, and many other disciplines. We will introduce three applications in this section: the use of congruences to assign memory locations to computer files, the generation of pseudorandom numbers, and check digits.

Suppose that a customer identification number is ten digits long. To retrieve customer files quickly, we do not want to assign a memory location to a customer record using the ten-digit identification number. Instead, we want to use a smaller integer associated to the identification number. This can be done using what is known as a hashing function. In this section we will show how we can use modular arithmetic to do hashing.

Constructing sequences of random numbers is important for randomized algorithms, for simulations, and for many other purposes. Constructing a sequence of truly random numbers is extremely difficult, or perhaps impossible, because any method for generating what are supposed to be random numbers may generate numbers with hidden patterns. As a consequence, methods have been developed for finding sequences of numbers that have many desirable properties of random numbers, and which can be used for various purposes in place of random numbers. In this section we will show how to use congruences to generate sequences of pseudorandom numbers. The advantage is that the pseudorandom numbers so generated are constructed quickly; the disadvantage is that they have too much predictability to be used for many tasks.

Congruences also can be used to produce check digits for identification numbers of various kinds, such as code numbers used to identify retail products, numbers used to identify books, airline ticket numbers, and so on. We will explain how to construct check digits using congruences for a variety of types of identification numbers. We will show that these check digits can be used to detect certain kinds of common errors made when identification numbers are printed.

### Hashing Functions



The central computer at an insurance company maintains records for each of its customers. How can memory locations be assigned so that customer records can be retrieved quickly? The solution to this problem is to use a suitably chosen **hashing function**. Records are identified using a **key**, which uniquely identifies each customer's records. For instance, customer records are often identified using the Social Security number of the customer as the key. A hashing function  $h$  assigns memory location  $h(k)$  to the record that has  $k$  as its key.

In practice, many different hashing functions are used. One of the most common is the function

$$h(k) = k \bmod m$$

where  $m$  is the number of available memory locations.

Hashing functions should be easily evaluated so that files can be quickly located. The hashing function  $h(k) = k \bmod m$  meets this requirement; to find  $h(k)$ , we need only compute the remainder when  $k$  is divided by  $m$ . Furthermore, the hashing function should be onto, so that all memory locations are possible. The function  $h(k) = k \bmod m$  also satisfies this property.

These last two congruences hold because  $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$  and  $11 \nmid ja$ , because  $11 \nmid j$  and  $11 \nmid a$ . We conclude that  $y_1 y_2 \dots y_{10}$  is not a valid ISBN. So, we have detected the single error.

Now suppose that two unequal digits have been transposed. It follows that there are distinct integers  $j$  and  $k$  such that  $y_j = x_k$  and  $y_k = x_j$ , and  $y_i = x_i$  for  $i \neq j$  and  $i \neq k$ . Hence,

$$\sum_{i=1}^{10} i y_i = \left( \sum_{i=1}^{10} i x_i \right) + (j x_k - j x_j) + (k x_j - k x_k) \equiv (j - k)(x_k - x_j) \not\equiv 0 \pmod{11},$$

because  $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$  and  $11 \nmid (j - k)$  and  $11 \nmid (x_k - x_j)$ . We see that  $y_1 y_2 \dots y_{10}$  is not a valid ISBN. Thus, we can detect the interchange of two unequal digits.

## Exercises

- Which memory locations are assigned by the hashing function  $h(k) = k \bmod 97$  to the records of insurance company customers with these Social Security numbers?
  - 034567981
  - 183211232
  - 220195744
  - 987255335
- Which memory locations are assigned by the hashing function  $h(k) = k \bmod 101$  to the records of insurance company customers with these Social Security numbers?
  - 104578690
  - 432222187
  - 372201919
  - 501338753
- A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function  $h(k) = k \bmod 31$ , where  $k$  is the number formed from the first three digits on a visitor's license plate.
  - Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310?
  - Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

Another way to resolve collisions in hashing is to use *double hashing*. We use an initial hashing function  $h(k) = k \bmod p$  where  $p$  is prime. We also use a second hashing function  $g(k) = (k + 1) \bmod (p - 2)$ . When a collision occurs, we use a *probing sequence*  $h(k, i) = (h(k) + i \cdot g(k)) \bmod p$ .

- Use the double hashing procedure we have described with  $p = 4969$  to assign memory locations to files for employees with social security numbers  $k_1 = 132489971$ ,  $k_2 = 509496993$ ,  $k_3 = 546332190$ ,  $k_4 = 034367980$ ,  $k_5 = 047900151$ ,  $k_6 = 329938157$ ,  $k_7 = 212228844$ ,  $k_8 = 325510778$ ,  $k_9 = 353354519$ ,  $k_{10} = 053708912$ .
- What sequence of pseudorandom numbers is generated using the linear congruential generator  $x_{n+1} = (3x_n + 2) \bmod 13$  with seed  $x_0 = 1$ ?
- What sequence of pseudorandom numbers is generated using the linear congruential generator  $x_{n+1} = (4x_n + 1) \bmod 7$  with seed  $x_0 = 3$ ?

- What sequence of pseudorandom numbers is generated using the pure multiplicative generator  $x_{n+1} = 3x_n \bmod 11$  with seed  $x_0 = 2$ ?
- Write an algorithm in pseudocode for generating a sequence of pseudorandom numbers using a linear congruential generator.

The **middle-square method** for generating pseudorandom numbers begins with an  $n$ -digit integer. This number is squared, initial zeros are appended to ensure that the result has  $2n$  digits, and its middle  $n$  digits are used to form the next number in the sequence. This process is repeated to generate additional terms.

- Find the first eight terms of the sequence of four-digit pseudorandom numbers generated by the middle square method starting with 2357.
- Explain why both 3792 and 2916 would be bad choices for the initial term of a sequence of four-digit pseudorandom numbers generated by the middle square method.

The **power generator** is a method for generating pseudorandom numbers. To use the power generator, parameters  $p$  and  $d$  are specified, where  $p$  is a prime,  $d$  is a positive integer such that  $p \nmid d$ , and a seed  $x_0$  is specified. The pseudorandom numbers  $x_1, x_2, \dots$  are generated using the recursive definition  $x_{n+1} = x_n^d \bmod p$ .

- Find the sequence of pseudorandom numbers generated by the power generator with  $p = 7$ ,  $d = 3$ , and seed  $x_0 = 2$ .
- Find the sequence of pseudorandom numbers generated by the power generator with  $p = 11$ ,  $d = 2$ , and seed  $x_0 = 3$ .
- Suppose you received these bit strings over a communications link, where the last bit is a parity check bit. In which string are you sure there is an error?
  - 00000111111
  - 10101010101
  - 11111100000
  - 10111101111
- Prove that a parity check bit can detect an error in a string if and only if the string contains an odd number of errors.

15. The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881. What is the check digit for that book?
  16. The ISBN-10 of the sixth edition of *Elementary Number Theory and Its Applications* is 0-321-500Q1-8, where  $Q$  is a digit. Find the value of  $Q$ .
  17. Determine whether the check digit of the ISBN-10 for this textbook (the seventh edition of *Discrete Mathematics and its Applications*) was computed correctly by the publisher.
- The United States Postal Service (USPS) sells money orders identified by an 11-digit number  $x_1x_2 \dots x_{11}$ . The first ten digits identify the money order;  $x_{11}$  is a check digit that satisfies  $x_{11} = x_1 + x_2 + \dots + x_{10} \pmod{9}$ .
18. Find the check digit for the USPS money orders that have identification number that start with these ten digits.
    - a) 7555618873
    - b) 6966133421
    - c) 8018927435
    - d) 3289744134
  19. Determine whether each of these numbers is a valid USPS money order identification number.
    - a) 74051489623
    - b) 88382013445
    - c) 56152240784
    - d) 66606631178
  20. One digit in each of these identification numbers of a postal money order is smudged. Can you recover the smudged digit, indicated by a  $Q$ , in each of these numbers?
    - a)  $Q1223139784$
    - b)  $6702120Q988$
    - c)  $27Q41007734$
    - d)  $213279032Q1$
  21. One digit in each of these identification numbers of a postal money order is smudged. Can you recover the smudged digit, indicated by a  $Q$ , in each of these numbers?
    - a)  $493212Q0688$
    - b)  $850Q9103858$
    - c)  $2Q941007734$
    - d)  $66687Q03201$
  22. Determine which single digit errors are detected by the USPS money order code.
  23. Determine which transposition errors are detected by the USPS money order code.
  24. Determine the check digit for the UPCs that have these initial 11 digits.
    - a) 73232184434
    - b) 63623991346
    - c) 04587320720
    - d) 93764323341
  25. Determine whether each of the strings of 12 digits is a valid UPC code.

- a) 036000291452
- b) 012345678903
- c) 782421843014
- d) 726412175425

26. Does the check digit of a UPC code detect all single errors? Prove your answer or find a counterexample.
27. Determine which transposition errors the check digit of a UPC code finds.

Some airline tickets have a 15-digit identification number  $a_1a_2 \dots a_{15}$  where  $a_{15}$  is a check digit that equals  $a_1a_2 \dots a_{14} \pmod{7}$ .

28. Find the check digit  $a_{15}$  that follows each of these initial 14 digits of an airline ticket identification number.
  - a) 10237424413392
  - b) 00032781811234
  - c) 00611232134231
  - d) 00193222543435
29. Determine whether each of these 15-digit numbers is a valid airline ticket identification number.
  - a) 101333341789013
  - b) 007862342770445
  - c) 113273438882531
  - d) 000122347322871
30. Which errors in a single digit of a 15-digit airline ticket identification number can be detected?
- \*31. Can the accidental transposition of two consecutive digits in an airline ticket identification number be detected using the check digit?

Periodicals are identified using an **International Standard Serial Number (ISSN)**. An ISSN consists of two blocks of four digits. The last digit in the second block is a check digit. This check digit is determined by the congruence  $d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}$ . When  $d_8 \equiv 10 \pmod{11}$ , we use the letter X to represent  $d_8$  in the code.

32. For each of these initial seven digits of an ISSN, determine the check digit (which may be the letter X).
  - a) 1570-868
  - b) 1553-734
  - c) 1089-708
  - d) 1383-811
33. Are each of these eight-digit codes possible ISSNs? That is, do they end with a correct check digit?
  - a) 1059-1027
  - b) 0002-9890
  - c) 1530-8669
  - d) 1007-120X
34. Does the check digit of an ISSN detect every single error in an ISSN? Justify your answer with either a proof or a counterexample.
35. Does the check digit of an ISSN detect every error where two consecutive digits are accidentally interchanged? Justify your answer with either a proof or a counterexample.