

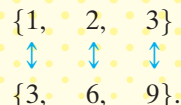
EXTENSION Infinite Sets and Their Cardinalities

One-to-One Correspondence and Equivalent Sets • The Cardinal Number \aleph_0
• Infinite Sets • Sets That Are Not Countable

One-to-One Correspondence and Equivalent Sets Georg Cantor met with much resistance in the late 1800s when he first developed modern set theory because of his ideas on infinite sets. The results discussed here, however, are commonly accepted today. Recall the following.

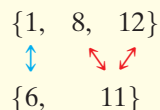
1. The cardinal number of a set is the number of elements it contains.
2. Two sets are *equivalent* if their cardinal numbers are equal.
3. A set is *infinite* if its cardinal number is “too large” to be found among the whole numbers.

We can easily establish the equivalence of two finite sets by counting their elements and comparing their cardinal numbers. But the elements of an infinite set cannot be counted in the same sense. Cantor addressed this difficulty using the idea of a **one-to-one correspondence** between sets. The sets $A = \{1, 2, 3\}$ and $B = \{3, 6, 9\}$, for example, can be placed in such correspondence as follows (among other ways):



This correspondence is “one-to-one” because each element of each set is paired with exactly one element of the other set. The equivalence of A and B is denoted $A \sim B$.

On the other hand, the sets $C = \{1, 8, 12\}$ and $D = \{6, 11\}$ are *not* equivalent. Any correspondence between them, such as



is not one-to-one. (Two different elements from C must be paired with a single element of D .)

Cantor extended this idea that one-to-one correspondence establishes equivalence to his study of infinite sets.

The Cardinal Number \aleph_0 The most basic infinite set is the set of counting numbers, $\{1, 2, 3, 4, 5, \dots\}$. The counting numbers are said to have the infinite cardinal number \aleph_0 (the first Hebrew letter, aleph, with a zero subscript, read “aleph-null”). Think of \aleph_0 as being the “smallest” infinite cardinal number. To the question “How many counting numbers are there?”, we answer “There are \aleph_0 of them.”

Now, any set that can be placed in a one-to-one correspondence with the counting numbers will have the same cardinal number, or \aleph_0 . There are many such sets.

EXAMPLE 1 Showing That $\{0, 1, 2, 3, \dots\}$ Has Cardinal Number \aleph_0

Verify that the set of whole numbers $\{0, 1, 2, 3, \dots\}$ has cardinal number \aleph_0 .

SOLUTION

We know that \aleph_0 is the cardinal number of the set of counting numbers (by definition). To show that another set, such as the whole numbers, also has \aleph_0 as its cardinal number, we must show that set to be equivalent to the set of counting numbers. Equivalence is established by a one-to-one correspondence between the two sets.



Aleph and other letters of the **Hebrew alphabet** are shown on a Kabbalistic diagram representing one of the ten emanations of God during Creation. Kabbalah, the ultramystical tradition within Judaism, arose in the fifth century and peaked in the sixteenth century in both Palestine and Poland.

Kabbalists believed that the Bible held mysteries that could be discovered in permutations, combinations, and anagrams of its very letters. Each letter in the aleph-bet has a numerical value (aleph = 1), and thus a numeration system exists. The letter Y stands for 10, so 15 should be YH (10 + 5). However, YH is a form of the Holy Name, so instead TW (9 + 6) is the symbol.

$$\begin{array}{ccccccccccc}
 \{1, & 2, & 3, & 4, & 5, & 6, & \dots, & n, & \dots\} & \text{Counting numbers} \\
 \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow \\
 \{0, & 1, & 2, & 3, & 4, & 5, & \dots, & n-1, & \dots\} & \text{Whole numbers}
 \end{array}$$

The pairing of the counting number n with the whole number $n - 1$ continues indefinitely, with neither set containing any element not used up in the pairing process. Even though the set of whole numbers has an additional element (the number 0) compared to the set of counting numbers, the correspondence proves that both sets have the same cardinal number, \aleph_0 . ■■■

The result in **Example 1** shows that intuition is a poor guide for dealing with infinite sets. Because the sets of counting numbers and whole numbers can be placed in a one-to-one correspondence, the two sets have the same cardinal number.

Infinite Sets The set $\{5, 6, 7\}$ is a proper subset of the set $\{5, 6, 7, 8\}$, and there is no way to place these two sets in a one-to-one correspondence. However, the set of counting numbers is a proper subset of the set of whole numbers, and **Example 1** showed that these two sets *can* be placed in a one-to-one correspondence. This important property is used in the formal definition of an infinite set.

Infinite Set

A set is **infinite** if it can be placed in a one-to-one correspondence with a proper subset of itself.

EXAMPLE 2 Showing That $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ Has Cardinal Number \aleph_0

Verify that the set of integers $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ has cardinal number \aleph_0 .

SOLUTION

A one-to-one correspondence can be set up between the set of integers and the set of counting numbers.

$$\begin{array}{ccccccccccccccc}
 \{1, & 2, & 3, & 4, & 5, & 6, & 7, & \dots, & 2n, & 2n+1, & \dots\} \\
 \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow \\
 \{0, & 1, & -1, & 2, & -2, & 3, & -3, & \dots, & n, & -n, & \dots\}
 \end{array}$$

Because of this one-to-one correspondence, the cardinal number of the set of integers is the same as the cardinal number of the set of counting numbers, \aleph_0 . ■■■

The one-to-one correspondence of **Example 2** proves that the set of integers is infinite—it was placed in one-to-one correspondence with a proper subset of itself.

As shown by **Example 2**, there are just as many integers as there are counting numbers. This result is not at all intuitive, and the next result is even less so. There is an infinite number of fractions between any two counting numbers. For example, there is an infinite set of fractions $\left\{\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \frac{15}{16}, \frac{31}{32}, \dots\right\}$ between the counting numbers 0 and 1. This should imply that there are “more” fractions than counting numbers. However, there are just as many fractions as counting numbers.

EXAMPLE 3 Showing That the Set of Rational Numbers Has Cardinal Number \aleph_0

Verify that the cardinal number of the set of rational numbers is \aleph_0 .

SOLUTION

First show that a one-to-one correspondence may be set up between the set of non-negative rational numbers and the counting numbers. This is done by the following ingenious scheme, devised by Georg Cantor.

Look at **Figure 22** on the next page. The nonnegative rational numbers whose denominators are 1 are written in the first row. Those whose denominators are 2 are written in the second row, and so on. Every nonnegative rational number appears in this list sooner or later. For example, $\frac{327}{189}$ is in row 189 and column 327.

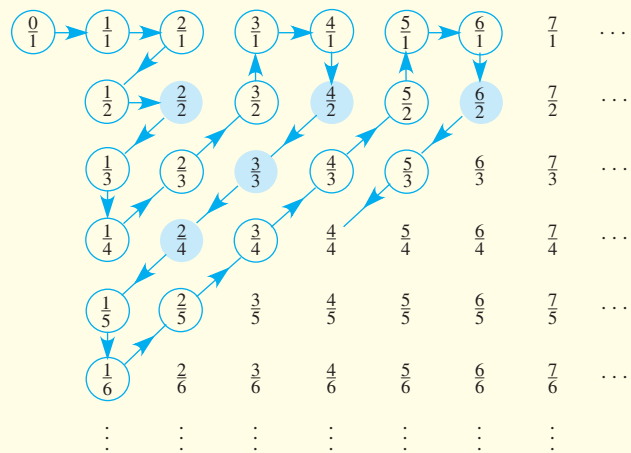


Figure 22

To set up a one-to-one correspondence between the set of nonnegative rationals and the set of counting numbers, follow the path drawn in **Figure 22**. Let $\frac{0}{1}$ correspond to 1, let $\frac{1}{1}$ correspond to 2, $\frac{2}{1}$ to 3, $\frac{1}{2}$ to 4 (skip $\frac{2}{2}$, since $\frac{2}{2} = \frac{1}{1}$), $\frac{1}{3}$ to 5, $\frac{1}{4}$ to 6, and so on. The numbers under the colored disks are omitted because they can be reduced to lower terms, and were thus included earlier in the listing.

This procedure sets up a one-to-one correspondence between the set of non-negative rationals and the counting numbers, showing that both of these sets have the same cardinal number, \aleph_0 . Now by using the method of **Example 2** (i.e., letting each negative number follow its corresponding positive number), we can extend this correspondence to include negative rational numbers as well. Thus, the set of all rational numbers has cardinal number \aleph_0 . ■■■

A set is called **countable** if it is finite or if it has cardinal number \aleph_0 . All the infinite sets of numbers discussed so far—the counting numbers, the whole numbers, the integers, and the rational numbers—are countable.

The Barber Paradox is a version of a paradox of set theory that Bertrand Russell proposed in the early twentieth century.

1. The men in a village are of two types: men who do not shave themselves and men who do.
2. The village barber shaves all men who do not shave themselves and he shaves only those men.

But who shaves the barber?

The barber cannot shave himself. If he did, he would fall into the category of men who shave themselves. However, (2) above states that the barber does not shave such men.

So the barber does not shave himself. But then he falls into the category of men who do not shave themselves. According to (2), the barber shaves all of these men; hence, the barber shaves himself, too.

We find that the barber cannot shave himself, yet the barber does shave himself—a paradox.

Sets That Are Not Countable

EXAMPLE 4

Showing That the Set of Real Numbers Does Not Have Cardinal Number \aleph_0

Verify that the set of all real numbers does not have cardinal number \aleph_0 .

SOLUTION

There are two possibilities:

1. The set of real numbers has cardinal number \aleph_0 .
2. The set of real numbers does not have cardinal number \aleph_0 .

If we assume that the first statement is true, then a one-to-one correspondence can be set up between the set of real numbers and the set of counting numbers.

In a later chapter, we show that every real number can be written as a decimal number (or simply “decimal”). Thus, in the one-to-one correspondence we are assuming, some decimal corresponds to the counting number 1, some decimal corresponds to 2, and so on. Suppose the correspondence begins as follows:

- 1 \leftrightarrow 0.68458429006 ...
 - 2 \leftrightarrow 0.13479201038 ...
 - 3 \leftrightarrow 0.37291568341 ...
 - 4 \leftrightarrow 0.935223671611 ...
- and so on.

Assuming the existence of a one-to-one correspondence between the counting numbers and the real numbers means that every decimal is in the list above. Let's construct a new decimal K as follows. The first decimal in the above list has 6 as its first digit. Let K start as $K = 0.4 \dots$. We picked 4 because $4 \neq 6$. (We could have used any other digit except 6.) Because the second digit of the second decimal in the list is 3, we let $K = 0.45 \dots$ (because $5 \neq 3$). The third digit of the third decimal is 2, so let $K = 0.457 \dots$ (because $7 \neq 2$). The fourth digit of the fourth decimal is 2, so let $K = 0.4573 \dots$ (because $3 \neq 2$). Continue defining K in this way.

Is K in the list that we assumed to contain all decimals? The first decimal in the list differs from K in at least the first position (K starts with 4, and the first decimal in the list starts with 6). The second decimal in the list differs from K in at least the second position, and the n th decimal in the list differs from K in at least the n th position. Every decimal in the list differs from K in at least one position, so that K cannot possibly be in the list. In summary:

We assume every decimal is in the list above.
The decimal K is not in the list.

Because these statements cannot both be true, the original assumption has led to a contradiction. This forces the acceptance of the only possible alternative to the original assumption: It is not possible to set up a one-to-one correspondence between the set of reals and the set of counting numbers. The cardinal number of the set of reals is not equal to \aleph_0 .

Zeno's paradox of the Tortoise and Achilles was given in its original form by Zeno of Elea.

In the original story, the Tortoise is able to convince Achilles (the Greek hero of Homer's *The Illiad*) that in a race, given a small head start, the Tortoise is always able to defeat Achilles. (See **Exercises 51 and 52** in this **Extension**.) The resolution of this paradox is discussed on the Web site www.mathacademy.com.

The set of counting numbers is a proper subset of the set of real numbers. Because of this, it would seem reasonable to say that the cardinal number of the set of reals, commonly written c , is greater than \aleph_0 . (The letter c here represents *continuum*.) Other, even larger, infinite cardinal numbers can be constructed. For example, the set of all subsets of the set of real numbers has a cardinal number larger than c . Continuing this process of finding cardinal numbers of sets of subsets, more and more, larger and larger infinite cardinal numbers are produced.

The six most important infinite sets of numbers were listed in the table below. All of them have been dealt with in this **Extension**, except the irrational numbers. The irrationals have decimal representations, so they are all included among the real numbers. Because the irrationals are a subset of the reals, you might guess that the irrationals have cardinal number \aleph_0 , just like the rationals. However, because the union of the rationals and the irrationals is all the reals, that would imply that the cardinality of the union of two disjoint countable sets is c . But **Example 2** showed that this is not the case. A better guess is that the cardinal number of the irrationals is c (the same as that of the reals). This is, in fact, true.

Cardinal Numbers of Infinite Number Sets

Infinite Set	Cardinal Number
Natural or counting numbers	\aleph_0
Whole numbers	\aleph_0
Integers	\aleph_0
Rational numbers	\aleph_0
Irrational numbers	c
Real numbers	c

EXTENSION EXERCISES

Match each set in Column I with the set in Column II that has the same cardinality. Give the cardinal number.

- | I | II |
|---|---|
| 1. $\{6\}$ | A. $\{x \mid x \text{ is a rational number}\}$ |
| 2. $\{-16, 14, 3\}$ | B. $\{26\}$ |
| 3. $\{x \mid x \text{ is a natural number}\}$ | C. $\{x \mid x \text{ is an irrational number}\}$ |
| 4. $\{x \mid x \text{ is a real number}\}$ | D. $\{x, y, z\}$ |
| 5. $\{x \mid x \text{ is an integer between 5 and 6}\}$ | E. $\{x \mid x \text{ is a real number that satisfies } x^2 = 25\}$ |
| 6. $\{x \mid x \text{ is an integer that satisfies } x^2 = 100\}$ | F. $\{x \mid x \text{ is an integer that is both even and odd}\}$ |

Place each pair of sets into a one-to-one correspondence, if possible.

7. $\{I, II, III\}$ and $\{x, y, z\}$
8. $\{a, b, c, d\}$ and $\{2, 4, 6\}$
9. $\{a, d, d, i, t, i, o, n\}$ and $\{a, n, s, w, e, r\}$
10. $\{\text{Obama, Clinton, Bush}\}$ and $\{\text{Michelle, Hillary, Laura}\}$

Give the cardinal number of each set.

11. $\{a, b, c, d, \dots, k\}$
12. $\{9, 12, 15, \dots, 36\}$
13. \emptyset
14. $\{0\}$
15. $\{300, 400, 500, \dots\}$
16. $\{-35, -28, -21, \dots, 56\}$
17. $\left\{-\frac{1}{4}, -\frac{1}{8}, -\frac{1}{12}, \dots\right\}$
18. $\{x \mid x \text{ is an even integer}\}$
19. $\{x \mid x \text{ is an odd counting number}\}$
20. $\{b, a, 1, 1, a, d\}$
21. $\{\text{Jan, Feb, Mar, } \dots, \text{Dec}\}$
22. $\{\text{Alabama, Alaska, Arizona, } \dots, \text{Wisconsin, Wyoming}\}$
23. Lew Lefton has revised the old song “100 Bottles of Beer on the Wall” to illustrate a property of infinite cardinal numbers.

Fill in the blank in the first verse of Lefton’s composition:

\aleph_0 bottles of beer on the wall, \aleph_0 bottles of beer,
take one down and pass it around, _____
bottles of beer on the wall.

(Source: <http://people.math.gatech.edu/~llefton>)



$$\aleph_0 - 1 = ?$$

(Photo courtesy of Joy Brown/Shutterstock.)

24. Two one-to-one correspondences are considered “different” if some elements are paired differently in one than in the other.

$\begin{matrix} \{a, & b, & c\} \\ \updownarrow & \updownarrow & \updownarrow \\ \{a, & b, & c\} \end{matrix}$	and	$\begin{matrix} \{a, & b, & c\} \\ \updownarrow & \updownarrow & \updownarrow \\ \{c, & b, & a\} \end{matrix}$	are different,
$\begin{matrix} \{a, & b, & c\} \\ \updownarrow & \updownarrow & \updownarrow \\ \{c, & a, & b\} \end{matrix}$	and	$\begin{matrix} \{b, & c, & a\} \\ \updownarrow & \updownarrow & \updownarrow \\ \{a, & b, & c\} \end{matrix}$	are not.

while

- (a) How many *different* correspondences can be set up between the two sets $\{\text{Jamie Foxx, Mike Myers, Madonna}\}$ and $\{\text{Austin Powers, Ray Charles, Eva Peron}\}$?
- (b) Which one of these correspondences pairs each person with the appropriate famous movie role?

Determine whether each pair of sets is equal, equivalent, both, or neither.

- | | |
|---|--------------------------------------|
| 25. $\{u, v, w\}, \{v, u, w\}$ | 26. $\{48, 6\}, \{4, 86\}$ |
| 27. $\{X, Y, Z\}, \{x, y, z\}$ | 28. $\{\text{top}\}, \{\text{pot}\}$ |
| 29. $\{x \mid x \text{ is a positive real number}\},$
$\{x \mid x \text{ is a negative real number}\}$ | |
| 30. $\{x \mid x \text{ is a positive rational number}\},$
$\{x \mid x \text{ is a negative real number}\}$ | |

Show that each set has cardinal number \aleph_0 by setting up a one-to-one correspondence between the given set and the set of counting numbers.

31. the set of positive even integers
32. $\{-10, -20, -30, -40, \dots\}$

33. $\{1,000,000, 2,000,000, 3,000,000, \dots\}$
34. the set of odd integers
35. $\{2, 4, 8, 16, 32, \dots\}$
(Hint: $4 = 2^2$, $8 = 2^3$, $16 = 2^4$, and so on)
36. $\{-17, -22, -27, -32, \dots\}$

In Exercises 37–40, identify the given statement as always true or not always true. If not always true, give a counterexample.

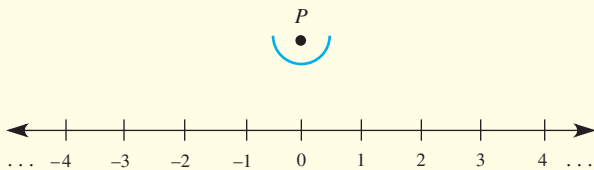
37. If A and B are infinite sets, then A is equivalent to B .
38. If set A is an infinite set and set B can be put in a one-to-one correspondence with a proper subset of A , then B must be infinite.
39. If A is an infinite set and A is not equivalent to the set of counting numbers, then $n(A) = c$.
40. If A and B are both countably infinite sets, then $n(A \cup B) = \aleph_0$

Exercises 41 and 42 are geometric applications of the concept of infinity.

41. The set of real numbers can be represented by an infinite line, extending indefinitely in both directions. Each point on the line corresponds to a unique real number, and each real number corresponds to a unique point on the line.

- (a) Use the figure below, where the line segment between 0 and 1 has been bent into a semicircle and positioned above the line, to prove that

$\{x | x \text{ is a real number between 0 and 1}\}$ is equivalent to $\{x | x \text{ is a real number}\}$.



- (b) What fact does part (a) establish about the set of real numbers?
42. Show that the two vertical line segments shown here both have the same number of points.



Show that each set can be placed in a one-to-one correspondence with a proper subset of itself to prove that the set is infinite.

43. $\{3, 6, 9, 12, \dots\}$
44. $\{4, 7, 10, 13, 16, \dots\}$
45. $\left\{\frac{3}{4}, \frac{3}{8}, \frac{3}{12}, \frac{3}{16}, \dots\right\}$
46. $\left\{1, \frac{4}{3}, \frac{5}{3}, 2, \dots\right\}$
47. $\left\{\frac{1}{9}, \frac{1}{18}, \frac{1}{27}, \frac{1}{36}, \dots\right\}$

48. $\{-3, -5, -9, -17, \dots\}$

49. Describe the distinction between *equal* and *equivalent* sets.

50. Explain how the correspondence suggested in **Example 4** shows that the set of real numbers between 0 and 1 is not countable.

The Paradoxes of Zeno Zeno was born about 496 B.C. in southern Italy. Two forms of his paradox are given below. What is your explanation for the following two examples of Zeno's paradoxes?

51. Achilles, if he starts out behind a tortoise, can never overtake the tortoise even if he runs faster.

Suppose Tortoise has a head start of one meter and goes one-tenth as fast as Achilles. When Achilles reaches the point where Tortoise started, Tortoise is then one-tenth meter ahead. When Achilles reaches *that* point, Tortoise is one-hundredth meter ahead. And so on. Achilles gets closer but can never catch up.

52. Motion itself cannot occur.

You cannot travel one meter until after you have first gone a half meter. But you cannot go a half meter until after you have first gone a quarter meter. And so on. Even the tiniest motion cannot occur because a tinier motion would have to occur first.

EXTENSION Modular Systems

Clock Arithmetic • Modular Systems • Residues of Large Numbers

Clock Arithmetic The numeration systems already discussed in this chapter all begin with the infinite set of whole numbers (or perhaps natural numbers), then devise ways to represent them, and use them for counting, calculating, and so on. There are many applications, however, where it is useful somehow to “reduce” the infinite set of numbers to a finite set. For example, consider this question:

Suppose it is 8 o'clock right now. What time will it be 33 hours from now?

Considering hours only (no minutes or seconds), any such question should have its answer in the finite set

$$\{1, 2, 3, \dots, 12\}.$$

But how is the answer found? One way is to use a 12-hour clock face, as in **Figure 12**, where 12 is replaced by 0 and the finite set for our 12-hour clock system is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Place the hour hand at 8. Then rotate it clockwise through a 33-hour arc. Wherever it stops is the answer. (Check that it is 5 o'clock.) **Example 1** shows another option, not using the clock face.



Figure 12

EXAMPLE 1 Computing a Sum in 12-Hour Clock Arithmetic

In 12-hour clock arithmetic, find the sum $8 + 33$.

SOLUTION

Use a calculator, and observe that

$$8 + 33 = 41 \quad \text{and} \quad \frac{41}{12} = 3.416666667.*$$

We don't care about the whole number of trips around the clock face, so drop the 3. Then multiply by 12 (and round if necessary) to obtain the remainder.

$$3.416666667 - 3 = 0.416666667$$

$$12 \cdot 0.416666667 = 5 \quad \leftarrow \text{The remainder is the answer.}$$

In 12-hour clock arithmetic, $8 + 33 = 5$. Thus, we have found that

$$8 + 33 = 3 \cdot 12 + 5,$$

which you can check directly. ■■■

Dividing any whole number by 12 will always yield a remainder in the set

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Thus the answer to any 12-hour clock arithmetic problem will be in this finite set. Every whole number, no matter how large, is “equivalent” to exactly one of these 12 remainders.

Plagued by serious maritime mishaps linked to navigational difficulties, several European governments offered prizes for an effective method of determining longitude. The largest prize was 20,000 pounds (equivalent to several million dollars in today's currency) offered by the British Parliament in the Longitude Act of 1714. While famed scientists, academics, and politicians pursued an answer in the stars, **John Harrison**, a clock maker, set about to build a clock that could maintain accuracy at sea. This turned out to be the key, and Harrison's **Chronometer** eventually earned him the prize.

For a fascinating account of this drama and of Harrison's struggle to collect his prize money from the government, see the book *The Illustrated Longitude* by Dava Sobel and William J. H. Andrewes.

*The equals symbol, $=$, is used in computations in this section despite the fact that some of the quotients are actually approximations.

EXAMPLE 2 Computing a Product in 12-Hour Clock Arithmetic

In 12-hour clock arithmetic, find the product $547 \cdot 11,873$.

SOLUTION

$$547 \cdot 11,873 = 6,494,531$$

$$\frac{6,494,531}{12} = 541,210.9167$$

$$12 \cdot 0.9167 = 11 \leftarrow \text{The remainder is the answer.}$$

In 12-hour clock arithmetic, $547 \cdot 11,873 = 11$. ■■■

EXAMPLE 3 Applying a 7-day “Clock”

Suppose that today is Thursday, January 15, 2015. What will be the day of the week exactly one year from today?

SOLUTION

Because 2015 is not divisible by 4, it is not a leap year so it has 365 days. In this case we need the remainder after 365 is divided by 7. We could rotate the “day hand” on the 7-day clock face in **Figure 13** or calculate as follows.

$$\frac{365}{7} = 52.14285714 \quad \text{and} \quad 52.14285714 - 52 = 0.14285714$$

$$7 \cdot 0.14285714 = 1$$

One year from today will be one day past Thursday—that is, Friday. ■■■

In this 7-day clock system, every whole number, no matter how large, is equivalent to exactly one remainder in the set $\{0, 1, 2, 3, 4, 5, 6\}$.

Modular Systems The many applications of such systems, which reduce the infinite set of whole numbers to a finite subset, based on remainders, have prompted mathematicians to expand these ideas to **modular systems** in general. **Example 3** showed that, in the 7-day clock system, 365 and 1 are, in a sense, equivalent. More formally, we say that 365 and 1 are **congruent modulo 7** (or **congruent mod 7**), which is written

$$365 \equiv 1 \pmod{7} \quad \text{The sign } \equiv \text{ indicates congruence.}$$

By observing 7-day clock hand movements, we also see that, for example,

$$8 \equiv 1 \pmod{7}, \quad 15 \equiv 1 \pmod{7}, \quad \text{and so on.}$$

In each case, the congruence is true because the difference of the two congruent numbers is a multiple of 7.

$$8 - 1 = 7 = 1 \cdot 7, \quad 15 - 1 = 14 = 2 \cdot 7, \quad 365 - 1 = 364 = 52 \cdot 7$$

Congruence Modulo n

The integers a and b are **congruent modulo n** (where n is a natural number greater than 1 called the **modulus**) if and only if the difference $a - b$ is divisible by n . Symbolically, this congruence is written as follows.

$$a \equiv b \pmod{n}$$

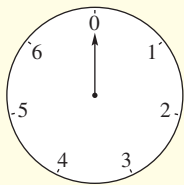


Figure 13

Because being divisible by n is the same as being a multiple of n , we can say that

$$a \equiv b \pmod{n} \text{ if and only if } a - b = kn \text{ for some integer } k.$$

EXAMPLE 4 Checking the Truth of Modular Equations

Decide whether each statement is *true* or *false*.

(a) $16 \equiv 10 \pmod{2}$ (b) $49 \equiv 32 \pmod{5}$ (c) $30 \equiv 345 \pmod{7}$

SOLUTION

- (a) The difference $16 - 10 = 6$ is divisible by 2, so $16 \equiv 10 \pmod{2}$ is *true*.
(b) The statement $49 \equiv 32 \pmod{5}$ is *false*, because $49 - 32 = 17$, which is not divisible by 5.
(c) The statement $30 \equiv 345 \pmod{7}$ is *true*, because $30 - 345 = -315$ is divisible by 7. (It doesn't matter if we find $30 - 345$ or $345 - 30$.)

A **chess clock** or double clock is used to time chess, backgammon, and Scrabble games. Push one button, and that clock stops—the other begins simultaneously. When a player's allotted time for the game has expired, that player will lose if he or she has not made the required number of moves.

Emanuel Lasker achieved mastery in both mathematics and chess. He was best known as a World Chess Champion for 27 years, until 1921. Lasker also was famous in mathematical circles for his work concerning the theory of primary ideals, algebraic analogies of prime numbers. The **Lasker-Noether theorem** bears his name along with that of **Emmy Noether**. Noether extended Lasker's work. Her father had been Lasker's Ph.D. advisor.

There is another method of determining if two numbers, a and b , are congruent modulo n .

Criterion for Congruence

$a \equiv b \pmod{n}$ if and only if the same remainder is obtained when a and b are divided by n .

For example, we know that $27 \equiv 9 \pmod{6}$ because $27 - 9 = 18$, which is divisible by 6. Now, if 27 is divided by 6, the quotient is 4 and the remainder is 3. Also, if 9 is divided by 6, the quotient is 1 and the remainder is 3. According to the criterion above, $27 \equiv 9 \pmod{6}$ since both remainders are the same.

Addition, subtraction, and multiplication can be performed in any modular system. Because final answers should be whole numbers less than the modulus, we can first find an answer using ordinary arithmetic. Then, as long as the answer is nonnegative, simply divide it by the modulus and keep the remainder. This produces the least nonnegative integer that is congruent (modulo n) to the ordinary answer.

EXAMPLE 5 Performing Modular Arithmetic

Find each sum, difference, or product.

(a) $(50 + 34) \pmod{7}$ (b) $(27 - 5) \pmod{6}$ (c) $(8 \cdot 9) \pmod{10}$

SOLUTION

- (a) First add 50 and 34 to get 84. Then divide 84 by 7. The remainder is 0, so we obtain $84 \equiv 0 \pmod{7}$ and
$$(50 + 34) \equiv 0 \pmod{7}.$$

(b) $27 - 5 = 22$. Divide 22 by 6, obtaining 4 as a remainder.
$$(27 - 5) \equiv 4 \pmod{6}$$

(c) Since $8 \cdot 9 = 72$, and 72 leaves a remainder of 2 when divided by 10,
$$(8 \cdot 9) \equiv 2 \pmod{10}.$$

PROBLEM-SOLVING HINT A modular system (mod n) allows only a fixed set of remainder values, $0, 1, 2, \dots, n - 1$. One practical approach to solving modular equations, at least when n is reasonably small, is to simply try all these integers. For each solution found in this way, others can be found by adding multiples of the modulus to it.

EXAMPLE 6 Solving Modular Equations

Solve each modular equation for whole number solutions.

(a) $(3 + x) \equiv 5 \pmod{7}$ (b) $5x \equiv 4 \pmod{9}$

(c) $6x \equiv 3 \pmod{8}$ (d) $8x \equiv 8 \pmod{8}$

SOLUTION

- (a) Because dividing 5 by 7 yields remainder 5, the criterion for congruence is that the given equation is true only if dividing $3 + x$ by 7 also yields remainder 5. Try replacing x , in turn, by 0, 1, 2, 3, 4, 5, and 6.

$x = 0$: $(3 + 0) \equiv 5 \pmod{7}$ is false. The remainder is 3.

$x = 1$: $(3 + 1) \equiv 5 \pmod{7}$ is false. The remainder is 4.

$x = 2$: $(3 + 2) \equiv 5 \pmod{7}$ is true. The remainder is 5.

Try $x = 3, x = 4, x = 5$, and $x = 6$ to see that none work. Of the integers from 0 through 6, only 2 is a solution of the equation $(3 + x) \equiv 5 \pmod{7}$.

Because 2 is a solution, find other solutions to this mod 7 equation by repeatedly adding 7.

$$2 + 7 = 9, \quad 9 + 7 = 16, \quad 16 + 7 = 23, \quad \text{and so on.}$$

The set of all nonnegative solutions of $(3 + x) \equiv 5 \pmod{7}$ is

$$\{2, 9, 16, 23, 30, 37, \dots\}.$$

- (b) Dividing 4 by 9 yields remainder 4. Because the modulus is 9, check the remainders when $5x$ is divided by 9 for $x = 0, 1, 2, 3, 4, 5, 6, 7$, and 8.

$x = 0$: $5 \cdot 0 \equiv 4 \pmod{9}$ is false. The remainder is 0.

$x = 1$: $5 \cdot 1 \equiv 4 \pmod{9}$ is false. The remainder is 5.

Continue trying numbers. Only $x = 8$ works.

$$5 \cdot 8 = 40 \equiv 4 \pmod{9} \quad \text{The remainder is 4.}$$

The set of all nonnegative solutions to the equation $5x \equiv 4 \pmod{9}$ is

$$\{8, 8 + 9, 8 + 9 + 9, 8 + 9 + 9 + 9, \dots\}, \quad \text{or} \quad \{8, 17, 26, 35, 44, 53, \dots\}.$$

- (c) To solve $6x \equiv 3 \pmod{8}$, try the numbers 0, 1, 2, 3, 4, 5, 6, and 7. None work. Therefore, the equation $6x \equiv 3 \pmod{8}$ has no solutions. Write the set of all solutions as the empty set, \emptyset .

This result is reasonable because $6x$ will always be even, no matter which whole number is used for x . Because $6x$ is even and 3 is odd, the difference $6x - 3$ will be odd and therefore not divisible by 8.

- (d) To solve $8x \equiv 8 \pmod{8}$, try the numbers 0, 1, 2, 3, 4, 5, 6, and 7. Any replacement will work. The solution set is $\{0, 1, 2, 3, \dots\}$, the set of all whole numbers. ■■■

Some problems can be solved by writing down two or more modular equations and finding their common solutions, as in the next example.

EXAMPLE 7 Finding the Number of Discs in a CD Collection

Julio wants to arrange his CD collection in equal size stacks, but after trying stacks of 4, stacks of 5, and stacks of 6, he finds that there is always 1 disc left over. Assuming Julio owns more than one CD, what is the least possible number of discs in his collection?

SOLUTION

The given information leads to three modular equations,

$$x \equiv 1 \pmod{4}, \quad x \equiv 1 \pmod{5}, \quad \text{and} \quad x \equiv 1 \pmod{6}.$$

For the first equation, try $x = 0, x = 1, x = 2$, and $x = 3$. The value 1 works, as it does for the other two equations as well. So the solution sets are, respectively,

$$\{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, \dots\},$$

$$\{1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, 61, 66, 71, 76, \dots\},$$

and $\{1, 7, 13, 19, 25, 31, 37, 43, 49, 55, 61, \dots\}.$

The least common solution greater than 1 is 61, so the least possible number of discs in the collection is 61. ■■■

EXAMPLE 8 Applying Congruences to a Construction Problem

Jeanne Bronson, a dry-wall contractor, is ordering materials to finish a 17-foot-by-45-foot room. The wallboard panels come in 4-foot widths. Show that, after uncut panels are applied, all four walls will require additional partial strips of the same width.

SOLUTION

The width of any partial strip needed will be the remainder when the wall length is divided by 4 (the panel width). In terms of congruence, we must show that $17 \equiv 45 \pmod{4}$. By the criterion for congruence, we see that this is true because both 17 and 45 give the same remainder (namely 1) when divided by 4. A 1-foot partial strip will be required for each wall. (In this case, Jeanne can use four 1-foot strips, cut from a single panel, so there will be no waste.) ■■■

Residues of Large Numbers The basic concern in a modular system with modulus n is

Given any whole number a , no matter how large, find the number b in the set

$$\{0, 1, 2, 3, \dots, n - 1\} \text{ such that } a \equiv b \pmod{n}.$$

This number b is the *remainder* when a is divided by n . It is called the **residue** of a , modulo n . To find this residue can be thought of as to “mod.” To mod a very large number a , we should definitely make use of a calculator. In fact, many modern applications involve huge numbers and require powerful computers and sophisticated algorithms to complete the process. (For example, see **Extension Modern Cryptography**.)

The process used earlier can be summarized.

Calculator Routine for Finding the Residue of a , Modulo n

In a modular system, the residue modulo n for a number a can be found by completing these three steps, in turn.

Step 1 Divide a by the modulus n .

Step 2 Subtract the integer part of the quotient to obtain only the fractional part.

Step 3 Multiply the fractional part of the quotient by n .

The final result is the residue modulo n .

EXAMPLE 9 Finding the Modular Residue of a Large Number

Find the residue of 846,238,527, modulo 23.

SOLUTION

$$\frac{846,238,527}{23} = 36,792,979.434783 \quad (\text{Your calculator may not display this many decimal places.})$$

$$36,792,979.434783 - 36,792,979 = 0.434783$$

$$23 \cdot 0.434783 = \mathbf{10} \quad \leftarrow \text{residue}$$

The residue is 10. ($846,238,527 = 36,792,979 \cdot 23 + 10$.)

Suppose we want to calculate the product of 458,687 and 931,056, modulo 18. The calculator displays the answer in exponential form.

$$458,687 \cdot 931,056 = 4.270632835\text{E}11$$

Step 1, dividing by 18, yields $2.372573797\text{E}10$, and we can't tell what the integer part is for Step 2. To get around this difficulty, we can use the fact that, in general,

the residue of a product equals the product of the residues

and employ the maxim,

“mod before you multiply.”

EXAMPLE 10 Finding the Residue of a Large Product

Find the residue of $458,687 \cdot 931,056$, modulo 18.

SOLUTION

$$\frac{458,687}{18} = 25,482.61111 \quad \text{and} \quad \frac{931,056}{18} = 51,725.33333$$

$$25,482.61111 - 25,482 = 0.61111 \quad \text{and} \quad 51,725.33333 - 51,725 = 0.33333$$

$$0.61111 \cdot 18 = 11 \quad \text{and} \quad 0.33333 \cdot 18 = 6$$

Now the product of the individual residues is $11 \cdot 6 = 66$. Since 66 is still not less than 18, simply mod again.

$$\frac{66}{18} = 3.666 \dots, \quad 3.666 \dots - 3 = 0.666 \dots, \quad \text{and} \quad 18 \cdot 0.666 \dots = \mathbf{12}$$

The residue, modulo 18, of $458,687 \cdot 931,056$ is 12.

EXTENSION EXERCISES

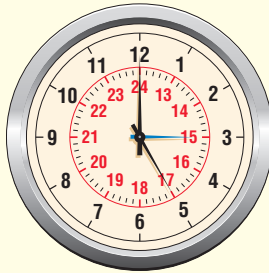
Find each sum or product in 12-hour clock arithmetic.

1. $7 + 16$
2. $3 + 21$
3. $9 \cdot 7$
4. $7 \cdot 11$

Find each sum or product in 7-day clock arithmetic.

5. $6 + 42$
6. $5 + 365$
7. $4 \cdot 28$
8. $3 \cdot 54$

The military uses a 24-hour clock to avoid the problems of “A.M.” and “P.M.” For example, 1100 hours is 11 A.M., while 2100 hours is 9 P.M. (12 noon + 9 hours). In these designations, the last two digits represent minutes, and the digits before that represent hours. Find each sum in the 24-hour clock system.



9. $1400 + 500$
10. $1300 + 1800$
11. $0750 + 1630$
12. $1545 + 0815$
13. Explain how the following three statements can *all* be true. (Hint: Think of clocks.)


$$\begin{aligned} 1145 + 1135 &= 2280 \\ 1145 + 1135 &= 1120 \\ 1145 + 1135 &= 2320 \end{aligned}$$

Answer true or false for each statement.

14. $5 \equiv 19 \pmod{3}$
15. $35 \equiv 8 \pmod{9}$
16. $5445 \equiv 0 \pmod{3}$
17. $7021 \equiv 4202 \pmod{6}$

Work each modular arithmetic problem.

18. $(12 + 7) \pmod{4}$
19. $(62 + 95) \pmod{9}$
20. $(35 - 22) \pmod{5}$
21. $(82 - 45) \pmod{3}$
22. $(5 \cdot 8) \pmod{3}$
23. $(32 \cdot 21) \pmod{8}$
24. $[4 \cdot (13 + 6)] \pmod{11}$
25. $[(10 + 7) \cdot (5 + 3)] \pmod{10}$

-  26. The text described how to do arithmetic mod n when the ordinary answer comes out nonnegative. Explain what to do when the ordinary answer is negative.

Find all nonnegative solutions for each equation.

27. $x \equiv 3 \pmod{7}$
28. $(2 + x) \equiv 7 \pmod{3}$
29. $6x \equiv 2 \pmod{2}$
30. $(5x - 3) \equiv 7 \pmod{4}$

Solve each problem.

31. **Odometer Readings** For many years automobile odometers showed five whole number digits and a digit for tenths of a mile. For those odometers showing just five whole number digits, totals are recorded according to what modulus?
32. **Distance Traveled by a Car** If a car's five-digit whole number odometer shows a reading of 29,306, in theory how many miles might the car have traveled?
33. **Silver Spoon Collection** Cheryl Falkowski has a collection of silver spoons from all over the world. She finds that she can arrange her spoons in sets of 7 with 6 left over, sets of 8 with 1 left over, or sets of 15 with 3 left over. If Cheryl has fewer than 200 spoons, how many are there?
34. **Piles of Ticket Stubs** Steven Booth finds that whether he sorts his White Sox ticket stubs into piles of 10, piles of 15, or piles of 20, there are always 2 left over. What is the least number of stubs he could have (assuming he has more than 2)?
35. **Flight Attendant Schedules** Megan Carvolth and Michele Dorsey, flight attendants for two different airlines, are close friends and like to get together as often as possible. Megan flies a 21-day schedule (including days off), which then repeats, while Michele has a repeating 30-day schedule. Both of their routines include layovers in Chicago, New Orleans, and San Francisco. The table below shows which days of each of their individual schedules they are in these cities. (Assume the first day of a cycle is day number 1.)

	Days in Chicago	Days in New Orleans	Days in San Francisco
Megan	1, 2, 8	5, 12	6, 18, 19
Michele	23, 29, 30	5, 6, 17	8, 10, 15, 20, 25

If today is July 1 and both are starting their schedules today (day 1), list the days during July and August that they will be able to see each other in each of the three cities.

The following formula can be used to find the day of the week on which a given year begins.* Here y represents the year (which must be after 1582, when our current calendar began). First calculate

$$a = y + \lfloor (y - 1)/4 \rfloor - \lfloor (y - 1)/100 \rfloor + \lfloor (y - 1)/400 \rfloor,$$

where, in general, $\lfloor x \rfloor$ is the greatest integer less than or equal to x . (For example, $\lfloor 9.2 \rfloor = 9$, and $\lfloor \pi \rfloor = 3$.) After finding a , find the smallest nonnegative integer b such that

$$a \equiv b \pmod{7}.$$

Then b gives the day of January 1, with $b = 0$ representing Sunday, $b = 1$ Monday, and so on.

Find the day of the week on which January 1 would occur in each year.

36. 1812 37. 1865 38. 2006 39. 2020

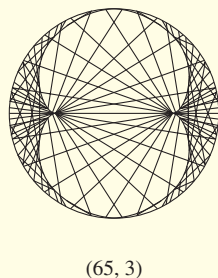
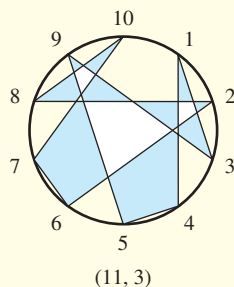
Some people believe that Friday the thirteenth is unlucky. The table* below shows the months that will have a Friday the thirteenth if the first day of the year is known. A year is a leap year if it is divisible by 4. The only exception to this rule is that a century year (1900, for example) is a leap year only when it is divisible by 400.

First Day of Year	Non-leap Year	Leap Year
Sunday	Jan., Oct.	Jan., April, July
Monday	April, July	Sept., Dec.
Tuesday	Sept., Dec.	June
Wednesday	June	March, Nov.
Thursday	Feb., March, Nov.	Feb., Aug.
Friday	August	May
Saturday	May	Oct.

Use the table to determine the months that have a Friday the thirteenth for each year.

40. 2011 41. 2012 42. 2013 43. 2200

44. Modular arithmetic can be used to create **residue designs**. For example, the designs (11, 3) and (65, 3) are shown here.



To see how such designs are created, construct a new design, (11, 5), by proceeding as follows.

- Draw a circle and divide the circumference into 10 equal parts. Label the division points as 1, 2, 3, ..., 10.
- Since $1 \cdot 5 \equiv 5 \pmod{11}$, connect 1 and 5. (We use 5 as a multiplier because we are making an (11, 5) design.)
- $2 \cdot 5 \equiv 10 \pmod{11}$
Therefore, connect 2 and ____.
- $3 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 3 and ____.
- $4 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 4 and ____.
- $5 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 5 and ____.
- $6 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 6 and ____.
- $7 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 7 and ____.
- $8 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 8 and ____.
- $9 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 9 and ____.
- $10 \cdot 5 \equiv \underline{\hspace{1cm}} \pmod{11}$
Connect 10 and ____.
- You might want to shade some of the regions you have found to make an interesting pattern. For more information, see "Residue Designs," by Phil Locke in *The Mathematics Teacher*, March 1972, pages 260–263.

Identification numbers are used in various ways for many kinds of different products. Books, for example, are assigned International Standard Book Numbers (ISBNs).

For many years, 10-digit ISBNs have been used. In 2007 a conversion process to 13 digits was begun. The 10-digit ISBN for this book is

0-321-69381-7.

The first digit, 0, identifies the book as being published in an English-language country. The next digits, 321, identify the publisher, and 69381 identifies this particular book. The final 7 is a check digit designed to help detect an invalid ISBN. (Maybe a wrong digit was entered, or two digits were inadvertently transposed.)

In general, if the digits are denoted $x_1, x_2, x_3, \dots, x_{10}$, then the check digit x_{10} is calculated using multipliers 1, 2, 3, 4, and so on up to 9, according to the following formula.

$$x_{10} = (1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9) \pmod{11}$$

*Given in "An Aid to the Superstitious," by G. L. Ritter, S. R. Lowry, H. B. Woodruff, and T. L. Isenhour. *The Mathematics Teacher*, May 1977, pp. 456–457.

For the ISBN 0-321-69381-7,

$$\begin{aligned}x_{10} &= (1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 6 + 6 \cdot 9 \\&\quad + 7 \cdot 3 + 8 \cdot 8 + 9 \cdot 1) \pmod{11} \\&= 194 \pmod{11} \\&= 7\end{aligned}$$

(If a check “digit” is 10, the letter X is used instead of 10.)

When an order for this book is received, the ISBN is entered into a computer, and the check (final digit on the right) digit evaluated. If this result does not match the check digit on the order, the order will not be processed.

Does each ISBN have the correct check digit?

45. 0-275-98341-2

46. 0-374-29288-7

Find the appropriate check digit for each ISBN. (Note: The positions of hyphens (or spaces) may vary (or there may be none). This does not affect the determination of the check digit.)

47. *Man of the Century*, by Jonathan Kwitny, 0-8050-2688- _____

48. *1776*, by David McCullough, 0-7432-2671- _____

For a 13-digit ISBN, find the check digit x_{13} as follows. First use alternating multipliers 1, 3, 1, 3, \dots , 1, 3 to determine the number

$$a = 1x_1 + 3x_2 + 1x_3 + 3x_4 + \cdots + 1x_{11} + 3x_{12}.$$

Then, if $a = 10$, $x_{13} = 0$. Otherwise, $x_{13} = 10 - a \pmod{10}$. Does each 13-digit ISBN have the correct check digit?

49. 978-0-06-193979-1

50. 978-1-4391-6857-8

Find the appropriate check digit for each ISBN.

51. *The Christmas Sweater*, by Glenn Beck, 978-1-4165-9485- _____

52. *One to Nine, The Inner Life of Numbers*, by Andrew Hodges, 978-0-393-33723- _____

Find the modular residue of each product.

53. $9,512,673 \cdot 2,583,691 \pmod{6}$

55. $14,501,302,706 \cdot 281,460,555 \pmod{19}$

56. $87,641,330 \cdot 21,376,486 \pmod{23}$

54. $369,852,142 \cdot 789,654,031 \pmod{9}$

EXTENSION Modern Cryptography

Basics of Cryptography • The Diffie-Hellman-Merkle Key Exchange Scheme
• RSA Public Key Cryptography

Basics of Cryptography Cryptography involves secret codes, ways of disguising information in order that a “sender” can transmit it to an intended “receiver” so that an “adversary” who somehow intercepts the transmission will be unable to discern its meaning. As is customary, we will refer to the sender and receiver (in either order) as Alice and Bob (A and B) and to the adversary as Eve (E). Converting a message to disguised form is called **encryption**, and converting it back to original form is called **decryption**.

Cryptography became more crucial as the extent of military, diplomatic, then industrial, and now even personal applications expanded. As the “code makers” became more adept at designing their systems, the “code breakers” became more adept at compromising those systems.

The basis of a cryptography system is normally some mathematical function, the “encryption algorithm,” that encrypts (disguises) the message. An example of a simple (and very insecure) encryption algorithm is the following:

Replace every letter of the alphabet with the letter that *follows* it.
(Replace z with a.)

Then the message “zebra” would be encrypted as “afcsb.” Analyzing one or more intercepted messages encrypted using this function, and trying various possibilities, would enable an adversary to quickly determine the function, and its inverse, which would be the following:

Replace every letter of the alphabet with the letter that *precedes* it.
(Replace a with z.)

More advanced systems also use a **key**, which is some additional information needed to perform the algorithm correctly. By the middle of the twentieth century, state-of-the-art requirements for an effective cryptography system were as follows.

Basic Requirements of a Cryptography System

1. A *secret* algorithm (or function) for encrypting and decrypting data
2. A *secret* key that provides additional information necessary for a receiver to carry out the decrypting process

The difficulty with requirement 1 was that all encryption functions at the time were two-way functions. Once an adversary obtained the encryption algorithm, the inverse (that is, the decryption algorithm) could be deduced mathematically.

The difficulty with requirement 2 was that the security of the key frequently dropped off after a period of use. This meant that Bob and Alice must exchange a new key fairly often so that their communications would continue to be safe. But this measure may be self-defeating, because every key exchange may be vulnerable to interception. This dilemma became known as the **key exchange problem** (or the **key distribution problem** in the case of multiple intended receivers).

In the 1970s, researchers discovered how to construct a *one-way* function that overcame both difficulties. It is an *exponential function*, and is given by

$$C = M^k \pmod{n},$$

with the calculation carried out modulo n . The achievement of an essentially one-way, rather than two-way, function, is made possible by the theory of large prime numbers, the nature of modular arithmetic (introduced in the **Extension Modular Systems**), and the present state of computer hardware and algorithms.

The Diffie-Hellman-Merkle Key Exchange Scheme First the key exchange problem was solved by the **Diffie-Hellman-Merkle key exchange scheme** (announced in 1976 and named for the Stanford University team of Whitfield Diffie, Martin Hellman, and Ralph Merkle). Basically, it works as follows.

The Diffie-Hellman-Merkle Key Exchange Scheme

Alice and Bob can establish a key (a number) that they both will know, but that Eve cannot find out, even if she observes the communications between Bob and Alice as they set up their key. Alice and Bob can agree to use the function $C = M^k \pmod{n}$ with specific values for M and n . (They can agree to all this by mail, telephone, e-mail, or even casual conversation. It won't matter if Eve finds out.) Then they carry out the following sequence of individual steps.

Alice's Actions

- Step 1** Choose a value of a .
(Keep this value secret.)
- Step 2** Compute $\alpha = M^a \pmod{n}$.
- Step 3** Send the value of α to Bob.
- Step 4** Receive the value of β from Bob.
- Step 5** Compute the key:
 $K = \beta^a \pmod{n}$.

Bob's Actions

- Step 1** Choose a value of b .
(Keep this value secret.)
- Step 2** Compute $\beta = M^b \pmod{n}$.
- Step 3** Send the value of β to Alice.
- Step 4** Receive the value of α from Alice.
- Step 5** Compute the key:
 $K = \alpha^b \pmod{n}$.

By this procedure, Alice and Bob will arrive at the same key value K because

$$\begin{aligned} \beta^a &= (M^b)^a & \beta &= M^b \\ &= M^{ba} & \text{Rule of exponents: } (a^m)^n &= a^{mn} \\ &= M^{ab} & \text{Commutative property: } ab &= ba \\ &= (M^a)^b & \text{Rule of exponents: } (a^m)^n &= a^{mn} \\ &= \alpha^b & \alpha &= M^a \end{aligned}$$

We illustrate the basic procedures using much smaller numbers than would be used in practice so that our computations can be done on a handheld calculator.

Modular arithmetic, as discussed in the Extension Modular Systems, will be essential here. Given a modulus n , every natural number a is “equivalent” (actually congruent) to the remainder obtained when a is divided by n . This remainder is called the residue of a , modulo n . To find the residue can be thought of as to “mod.”

16807/13	1292.846154
Ans-1292	.8461538462
Ans*13	11

The display shows that the residue of 16,807, modulo 13, is 11.

In **Example 1** to follow, for instance, one of the calculations will be to find the residue of 16,807, modulo 13. The calculator routine from the **Extension Modular Systems** applies as follows.

Step 1 Divide 16,807 by 13, obtaining 1292.846154.

Step 2 Subtract the integer part of the quotient, obtaining 0.846154. . .

Step 3 Multiply by 13, obtaining 11. (Round if necessary.)

So, we see that $16,807 \equiv 11 \pmod{13}$. We have shown that $16,807 = 1292 \cdot 13 + 11$.

(Note: In the work that follows, we carry out some lengthy sequences of modular arithmetic. We sometimes use the equals symbol, $=$, rather than the congruence symbol, \equiv , and when the modulus is understood, we sometimes omit the designation \pmod{n} .)

Calculator Routine for Finding the Residue of a , Modulo n

In a modular system, the residue modulo n for a number a can be found by completing these three steps, in turn.

Step 1 Divide a by the modulus n .

Step 2 Subtract the integer part of the quotient to obtain only the fractional part.

Step 3 Multiply the fractional part of the quotient by n .

The final result is the residue modulo n .

EXAMPLE 1 Using the Diffie-Hellman-Merkle Key Exchange Scheme

Establish a common key for Alice and Bob by using specific values for M , n , a , and b , and completing the steps outlined earlier for the Diffie-Hellman-Merkle key exchange scheme.

SOLUTION

Suppose Alice and Bob agree to use the values $M = 7$ and $n = 13$.

Alice's Actions

Step 1 Choose a value of a , say 5.
(Alice keeps this value secret.)

Step 2 $\alpha = M^a \pmod{n}$
 $= 7^5 \pmod{13}$
 $= 16,807 \pmod{13}$
 $= 11$

Step 3 Send $\alpha = 11$ to Bob.

Step 4 Receive $\beta = 3$.

Step 5 Compute the key:
 $K = \beta^a \pmod{n}$
 $= 3^5 \pmod{13}$
 $= 243 \pmod{13}$
 $= 9.$

Bob's Actions

Step 1 Choose a value of b , say 8.
(Bob keeps this value secret.)

Step 2 $\beta = M^b \pmod{n}$
 $= 7^8 \pmod{13}$
 $= 5,764,801 \pmod{13}$
 $= 3$

Step 3 Send $\beta = 3$ to Alice.

Step 4 Receive $\alpha = 11$.

Step 5 Compute the key:
 $K = \alpha^b \pmod{n}$
 $= 11^8 \pmod{13}$
 $= 214,358,881 \pmod{13}$
 $= 9.$

11^8	214358881
Ans/13	16489144.69
Ans-16489144	.692308
Ans*13	9.000004

The display shows the calculation of K in the right column. (Ignore the tiny roundoff error.)

Both Alice and Bob arrived at the same key value, $K = 9$, which they can use for encrypting future communications to one another. ■■■

When the **RSA code** was first introduced in 1977, Martin Gardner's "Mathematical Games" column in *Scientific American* challenged researchers to decode a message using an n with 129 digits. With the aid of number theory, it took 600 mathematicians in 25 different countries only 17 years to factor n into 64- and 65-digit prime factors, as shown here.

114,381,625,757,888,867,669,235,779,976,
146,612,010,218,296,721,242,362,562,561,
842,935,706,935,245,733,897,830,597,123,
563,958,705,058,989,075,147,599,290,026,
879,543,541 = 3,490,529,510,847,650,949,
147,849,619,903,898,133,417,764,638,493,
387,843,990,820,577 \times 32,769,132,993,
266,709,549,961,988,190,834,461,413,177,
642,967,992,942,539,798,288,533

The decoded message said, "The magic words are squeamish ossifrage."

Today, RSA users select much larger values of p and q , resulting in an n of well over 300 digits. It is thought that breaking such an encryption would take all the computers in the world, working together, more time than the age of the universe.

Suppose, at Step 3 in **Example 1**, Eve intercepts Bob's transmission of the value $\beta = 3$ to Alice. This will not help her, because she cannot deduce Bob's value of b that generated β . In fact it could have been any of the values

$$8, 20, 32, 44, 56, \dots,$$

an infinite list of possibilities. (In practice, all the numbers in this list would be vastly greater.) Also, Eve does not know what exponent Alice will apply to 3 to obtain the key. The value

$$a = 5$$

is Alice's secret, never communicated to anyone else, not even Bob, so Eve cannot know what key Alice will obtain. The same argument applies if Eve intercepts Alice's transmission to Bob of the value

$$\alpha = 11.$$

(She is stymied even if she intercepts both transmissions.)

RSA Public Key Cryptography At practically the same time that Diffie, Hellman, and Merkle solved the key exchange problem, another team of researchers, Ron Rivest, Adi Shamir, and Leonard Adleman, at MIT, used the same type of mathematical function to eliminate the need for key exchange. Their scheme, known as RSA (from their surnames), is called **public key cryptography**. Anyone who wants the capability of receiving encrypted data simply makes known their public key, which anyone else can then use to encrypt messages to them. The beauty of the system is that the receiver possesses another private key, necessary for decrypting but never released to anyone else.

What makes RSA successful is that we have the mathematical understanding to identify very large prime numbers, and to multiply them to obtain a product. But if the prime factors are large enough, it is impossible, given the present state of knowledge, for anyone to determine the two original factors, even using very powerful computers.

Using RSA, Alice can receive encrypted messages from Bob in such a way that Eve cannot discern their meaning even if she intercepts them. We show here a complete outline of all the basic procedures, from setting up the scheme to encrypting and then decrypting a message.

RSA Basics: A Public Key Cryptography Scheme

Alice (the receiver) completes the following steps.

Step 1 Choose two prime numbers, p and q , which she keeps secret.

Step 2 Compute the *modulus* n (which is the product $p \cdot q$).

Step 3 Compute $\ell = (p - 1)(q - 1)$.

Step 4 Choose the *encryption exponent* e , which can be any integer between 1 and ℓ that is relatively prime to ℓ , that is, has no common factors with ℓ .

Step 5 Find her *decryption exponent* d , a number satisfying

$$e \cdot d = 1 \pmod{\ell}.$$

She keeps d secret.

Step 6 Provide Bob with her *public key*, which consists of the modulus n and the encryption exponent e .

(Bob's steps are on the next page.)

RSA Basics: A Public Key Cryptography Scheme (Cont.)

Now Bob (the sender) completes the following steps. (Recall that the purpose of all this is for Bob to be able to send Alice secure messages.)

Step 7 Convert the message to be sent to Alice into a number M (sometimes called the *plaintext*).

Step 8 Encrypt M , that is, use Alice's public key (n and e) to generate the encrypted message C (sometimes called the *ciphertext*) according to the formula

$$C = M^e \pmod{n}.$$

Step 9 Transmit C to Alice.

When Alice receives C , she completes the final step:

Step 10 Decrypt C , that is, use her private key, consisting of n (also part of her public key) and d , to reproduce the original plaintext message M according to the formula

$$M = C^d \pmod{n}.$$

A **brilliant number** (defined only in the last few years) is a product of two primes with equal numbers of digits. Is the product n in **Example 2** brilliant?

EXAMPLE 2 Devising a Public Encryption Key

Use the values $p = 7$ and $q = 13$ (arbitrarily chosen primes) to devise Alice's public key by completing Steps 2–4 of the above outline of RSA basics.

SOLUTION

Step 2 $n = p \cdot q = 7 \cdot 13 = 91$

Step 3 $\ell = (p - 1)(q - 1) = 6 \cdot 12 = 72$

Step 4 There are many choices here, but a prime less than 72 and relatively prime to 72 will meet the requirements. We arbitrarily choose $e = 11$.

Alice's public key is $n = 91$, $e = 11$. (Prime factors p and q must be kept secret.)

EXAMPLE 3 Finding a Private Decryption Key

Complete Step 5 of the RSA basics outline to find Alice's private decryption key.

SOLUTION

Step 5 The decryption exponent d must satisfy

$$e \cdot d = 1 \pmod{\ell} \quad \text{or} \quad 11d = 1 \pmod{72}.$$

One way to satisfy this equation is to check the powers of 11 until we find one equal (actually congruent) to 1, modulo 72:

Mod 72
congruences

$$\begin{aligned} 11^1 &= 11, & 11^2 &= 121 = 49, & 11^3 &= 1331 = 35, \\ 11^4 &= 14,641 = 25, & 11^5 &= 161,051 = 59, & 11^6 &= 1,771,561 = 1. \end{aligned}$$

(The residues were found using the calculator routine given before **Example 1**.) Because we found that $11^6 = 1$, we take $d = 11^5 = 59$. This way,

$$e \cdot d = 11 \cdot 11^5 = 11^6 = 1, \quad \text{as required.}$$

Alice's private key is $n = 91$, $d = 59$.

James Ellis, Clifford Cocks, and Malcolm Williamson all worked for Britain's Government Communications Headquarters in the 1970s. They actually discovered the mathematics of public key cryptography several years before the work at Stanford and MIT was announced (and subsequently patented). The British work was classified top secret and never came to light until some twenty years later, at approximately the same time that RSA Data Security, the company that had been built on U.S. RSA patents, was sold for \$200 million.

EXAMPLE 4 Encrypting a Message for Transmission

Complete Steps 7 and 8 of the RSA basics outline to encrypt the message “HI” for Bob to send Alice. Use Alice’s public key found in **Example 2**: $n = 91$, $e = 11$.

SOLUTION

Step 7 A simple way to convert “HI” to a number is to note that H and I are the 8th and 9th letters of the English alphabet. Simply let the plaintext message be $M = 89$.

Step 8 Now compute the ciphertext C : $C = M^e \pmod{n} = 89^{11} \pmod{91}$.

Here, 89^{11} is too large to be handled as we did the powers of 11 in **Example 3**. But we can use a trick here, expressing 11 as $1 + 2 + 8$. (1, 2, and 8 are the unique powers of 2 that sum to 11. Now we can rewrite 89^{11} in terms of smaller powers and then make use of rules of exponents.

$$\begin{aligned} 89^{11} &= 89^{1+2+8} & 1 + 2 + 8 &= 11 \\ &= 89^1 \cdot 89^2 \cdot 89^8 & \text{Rule of exponents: } a^{n+m} &= a^n \cdot a^m \end{aligned}$$

Now we “mod before we multiply,” in other words, we compute the residue of individual factors first, then multiply those results. This keeps the numbers smaller.

$$\begin{aligned} 89^1 &= 89 & \text{Definition of first power} \\ 89^2 &= 7921 = 4 & \text{Mod} \\ 89^8 &= 3.936588806\text{E}15 & \text{Calculator result} \end{aligned}$$

This last factor is too large to handle like the others. Due to the way we “split up” the exponent, subsequent powers of 89 can be written as powers of earlier ones.

$$\begin{aligned} 89^8 &= (89^2)^4 & \text{Rule of exponents: } a^{m \cdot n} &= (a^m)^n \\ &= 4^4 & 89^2 &= 4 \text{ from above.} \\ &= 256 & \text{Evaluate } 4^4. \\ &= 74 & \text{Mod} \end{aligned}$$

Finally we obtain

$$\begin{aligned} 89^{11} &= 89 \cdot 4 \cdot 74 & \text{Substitute.} \\ &= 26,344 & \text{Multiply.} \\ &= 45. & \text{Mod} \end{aligned}$$

The plaintext $M = 89$ (for the message “HI”) has been converted to the ciphertext $C = 45$. ■■■

Let’s see if Alice can successfully decrypt the message 45 when she receives it.

EXAMPLE 5 Decrypting a Received Message

Complete Step 10 of the RSA basics outline to decrypt the message $C = 45$ from **Example 4**. Use Alice’s private key, found in **Example 3**: $d = 59$ (also, $n = 91$).

SOLUTION

Step 10 The decryption formula gives

$$\begin{aligned} M &= C^d \pmod{n} \\ &= 45^{59} \pmod{91} & \text{Substitute.} \\ &= 45^{1+2+8+16+32} \pmod{91} & \text{Use sum of powers of 2.} \\ &= 45 \cdot 45^2 \cdot 45^8 \cdot 45^{16} \cdot 45^{32} \pmod{91}. & \text{Rule of exponents: } a^{m+n} &= a^m \cdot a^n \end{aligned}$$

Start with the smaller powers and “mod” each factor individually.

$$45^2 = 2025 = 23$$

$$45^8 = (45^2)^4 = 23^4 = 279,841 = 16$$

$$45^{16} = (45^8)^2 = 16^2 = 256 = 74$$

$$45^{32} = (45^{16})^2 = 74^2 = 5476 = 16$$

Inserting these values in the product for M , we get

$$\begin{aligned} M &= 45 \cdot 23 \cdot 16 \cdot 74 \cdot 16 \\ &= 19,607,040 \\ &= 89. \end{aligned}$$

We have correctly decrypted $C = 45$ to obtain

$$M = 89 = \text{HI.}$$



EXTENSION EXERCISES

Find the residue in each case.

1. $45 \pmod{6}$
2. $67 \pmod{10}$
3. $225 \pmod{13}$
4. $418 \pmod{15}$
5. $5^9 \pmod{12}$
6. $4^{11} \pmod{9}$
7. $8^7 \pmod{11}$
8. $14^5 \pmod{13}$
9. $8^{27} \pmod{17}$
10. $45^7 \pmod{23}$
11. $11^{14} \pmod{18}$
12. $14^9 \pmod{19}$

Finding a Common Key Find Alice and Bob’s common key K by using the Diffie-Hellman-Merkle key exchange scheme with the given values of M , n , a , and b .

	M	n	a	b
13.	5	13	7	6
14.	11	9	5	4
15.	5	11	6	7
16.	17	5	6	3

Apply the RSA scheme to find each missing value.

	p	q	n	ℓ
17.	5	11	_____	_____
18.	11	3	_____	_____
19.	5	13	_____	_____
20.	17	7	_____	_____

Encrypting Plaintext Given the modulus n , the encryption exponent e , and the plaintext M , use RSA encryption to find the ciphertext C in each case.

	n	e	M
21.	55	7	15
22.	33	7	8
23.	65	5	16
24.	119	11	12

Decrypting Ciphertext Given the prime factors p and q , the encryption exponent e , and the ciphertext C , apply the RSA algorithm to find (a) the decryption exponent d and (b) the plaintext message M .

	p	q	e	C
25.	5	11	3	30
26.	11	3	13	24
27.	5	13	35	17
28.	17	7	5	40

29. Describe the breakthrough represented by Diffie-Hellman-Merkle and RSA as opposed to all earlier forms of cryptography.
30. Explain why RSA would fail if mathematicians could (using computers) factor arbitrarily large numbers.

EXTENSION Complex Numbers



Gauss and the Complex Numbers In about 1831 **Carl Gauss** was able to show that numbers of the form $a + bi$ can be represented as points on the plane just as real numbers are. He shared this contribution with **Robert Argand**, a bookkeeper in Paris, who wrote an essay on the geometry of the complex numbers in 1806. This went unnoticed at the time. (Image courtesy of Pearson Education, Inc.)

An Imaginary Tale: The Story of $\sqrt{-1}$ by Paul J. Nahin provides a historical account of the development of complex numbers.

Basic Concepts and the Imaginary Unit Numbers such as $\sqrt{-5}$ and $\sqrt{-16}$ were called *imaginary* by early mathematicians. Eventually, their use made it necessary to expand the set of real numbers to form the set of **complex numbers**.

Consider the equation $z^2 + 1 = 0$. It has no real number solution, since any solution must be a number whose square is -1 . In the set of real numbers all squares are nonnegative numbers, because the product of either two positive numbers or two negative numbers is positive and $0^2 = 0$. To provide a solution for the equation $z^2 + 1 = 0$, a new number i is defined so that the following is true.

$$i^2 = -1, \text{ which implies that } i = \sqrt{-1}.$$

The number i is called the **imaginary unit**. This definition of i makes it possible to define the square root of any negative number as follows.

$$\sqrt{-b}$$

For any positive real number b , $\sqrt{-b} = i\sqrt{b}$.

EXAMPLE 1 Writing Square Roots Using i

Write each number as a product of a real number and i .

(a) $\sqrt{-100}$ (b) $\sqrt{-2}$

SOLUTION

(a) $\sqrt{-100} = i\sqrt{100} = 10i$ (b) $\sqrt{-2} = \sqrt{2}i = i\sqrt{2}$

In **Example 1(b)**, it is easy to mistake $\sqrt{2}i$ for $\sqrt{2i}$, with the i under the radical. For this reason, it is common to write $\sqrt{2}i$ as $i\sqrt{2}$.

Products and Quotients When finding a product such as $\sqrt{-4} \cdot \sqrt{-9}$, the product rule for radicals cannot be used, since that rule applies only when both radicals represent real numbers. For this reason, always change $\sqrt{-b}$ (where $b > 0$) to the form $i\sqrt{b}$ before performing any multiplications or divisions.

$$\sqrt{-4} \cdot \sqrt{-9} = i\sqrt{4} \cdot i\sqrt{9} = i \cdot 2 \cdot i \cdot 3 = 6i^2$$

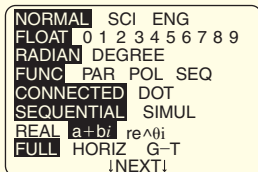
Since $i^2 = -1$,

$$6i^2 = 6(-1) = -6.$$

An **incorrect** use of the product rule for radicals would give a wrong answer.

$$\sqrt{-4} \cdot \sqrt{-9} = \sqrt{(-4)(-9)} = \sqrt{36} = 6 \quad \text{Incorrect}$$

This same reasoning holds for quotients as well.



When the TI-83/84 Plus calculator is in complex mode, denoted by $a + bi$, it will perform complex number arithmetic.

EXAMPLE 2 Multiplying Expressions Involving i

Multiply.

(a) $\sqrt{-3} \cdot \sqrt{-7}$ (b) $\sqrt{-2} \cdot \sqrt{-8}$ (c) $\sqrt{-5} \cdot \sqrt{6}$

SOLUTION

(a) $\sqrt{-3} \cdot \sqrt{-7} = i\sqrt{3} \cdot i\sqrt{7} = i^2\sqrt{3 \cdot 7} = (-1)\sqrt{21} = -\sqrt{21}$

(b) $\sqrt{-2} \cdot \sqrt{-8} = i\sqrt{2} \cdot i\sqrt{8} = i^2\sqrt{2 \cdot 8} = (-1)\sqrt{16} = (-1)4 = -4$

(c) $\sqrt{-5} \cdot \sqrt{6} = i\sqrt{5} \cdot \sqrt{6} = i\sqrt{30}$



EXAMPLE 3 Dividing Expressions Involving i

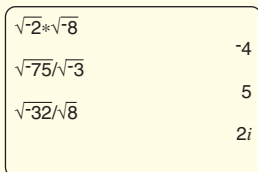
Divide.

(a) $\frac{\sqrt{-75}}{\sqrt{-3}}$ (b) $\frac{\sqrt{-32}}{\sqrt{8}}$

SOLUTION

(a) $\frac{\sqrt{-75}}{\sqrt{-3}} = \frac{i\sqrt{75}}{i\sqrt{3}} = \sqrt{\frac{75}{3}} = \sqrt{25} = 5$

(b) $\frac{\sqrt{-32}}{\sqrt{8}} = \frac{i\sqrt{32}}{\sqrt{8}} = i\sqrt{\frac{32}{8}} = i\sqrt{4} = 2i$



This screen supports the results of Examples 2(b), 3(a), and 3(b).

Complex Numbers and Powers of i Complex numbers are defined as follows.

Complex Numbers

If a and b are real numbers, then any number of the form $a + bi$ is called a **complex number**.

In the complex number $a + bi$, the number a is called the **real part** and b is called the **imaginary part**.^{*} When $b = 0$, $a + bi$ is a real number, so the real numbers are a subset of the complex numbers. Complex numbers of the form bi , where $b \neq 0$, are called **pure imaginary numbers**. In spite of their name, such numbers are very useful in applications, particularly in work with electricity.

An interesting pattern emerges when we consider various powers of i . By definition, $i^0 = 1$, and $i^1 = i$. We have seen that $i^2 = -1$, and greater powers of i can be found as shown in the following list.

$$i^3 = i \cdot i^2 = i(-1) = -i$$

$$i^6 = i^2 \cdot i^4 = (-1) \cdot 1 = -1$$

$$i^4 = i^2 \cdot i^2 = (-1)(-1) = 1$$

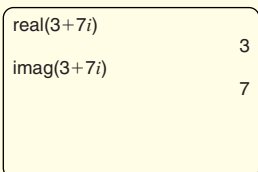
$$i^7 = i^3 \cdot i^4 = (-i) \cdot 1 = -i$$

$$i^5 = i \cdot i^4 = i \cdot 1 = i$$

$$i^8 = i^4 \cdot i^4 = 1 \cdot 1 = 1$$

A few powers of i are listed on the next page.

^{*}In some texts, bi is called the imaginary part.



The TI-83/84 Plus calculator identifies the real and imaginary parts of $3 + 7i$.

i^2	
i^3	-1
i^4	$-i$
	1

The calculator computes powers of i . Compare to the powers in the chart.

Powers of i

$i^1 = i$	$i^5 = i$	$i^9 = i$	$i^{13} = i$
$i^2 = -1$	$i^6 = -1$	$i^{10} = -1$	$i^{14} = -1$
$i^3 = -i$	$i^7 = -i$	$i^{11} = -i$	$i^{15} = -i$
$i^4 = 1$	$i^8 = 1$	$i^{12} = 1$	$i^{16} = 1$

The powers of i rotate through the four numbers i , -1 , $-i$, and 1 . Larger powers of i can be simplified by using the fact that $i^4 = 1$. For example, consider i^{75} .

$$i^{75} = (i^4)^{18} \cdot i^3 = 1^{18} \cdot i^3 = 1 \cdot i^3 = -i$$

Simplifying Large Powers of i

Step 1 Divide the exponent by 4.

Step 2 Observe the remainder obtained in Step 1. The large power of i is the same as i raised to the power determined by this remainder. Refer to the previous chart to complete the simplification. (If the remainder is 0, the power simplifies to $i^0 = 1$.)

EXAMPLE 4 Simplifying Powers of i

Simplify each power of i .

(a) i^{12} (b) i^{39}

SOLUTION

(a) $i^{12} = (i^4)^3 = 1^3 = 1$

(b) To find i^{39} , start by dividing 39 by 4 (Step 1), as shown in the margin. The remainder is 3. So $i^{39} = i^3 = -i$ (Step 2).

Another way to simplify i^{39} is as follows.

$$i^{39} = i^{36} \cdot i^3 = (i^4)^9 \cdot i^3 = 1^9 \cdot (-i) = -i$$

EXTENSION EXERCISES

Use the method of **Examples 1–3** to write each expression as a real number or a product of a real number and i .

- $\sqrt{-144}$
- $\sqrt{-196}$
- $-\sqrt{-225}$
- $-\sqrt{-400}$
- $\sqrt{-3}$
- $\sqrt{-19}$
- $\sqrt{-75}$
- $\sqrt{-125}$
- $\sqrt{-5} \cdot \sqrt{-5}$
- $\sqrt{-3} \cdot \sqrt{-3}$
- $\sqrt{-9} \cdot \sqrt{-36}$
- $\sqrt{-4} \cdot \sqrt{-81}$
- $\sqrt{-16} \cdot \sqrt{-100}$
- $\sqrt{-81} \cdot \sqrt{-121}$

15. $\frac{\sqrt{-200}}{\sqrt{-100}}$

17. $\frac{\sqrt{-54}}{\sqrt{6}}$

19. $\frac{\sqrt{-288}}{\sqrt{-8}}$

16. $\frac{\sqrt{-50}}{\sqrt{-2}}$

18. $\frac{\sqrt{-90}}{\sqrt{10}}$

20. $\frac{\sqrt{-48} \cdot \sqrt{-3}}{\sqrt{-2}}$

Use the method of **Example 4** to simplify each power of i .

- i^8
- i^{16}
- i^{42}
- i^{86}
- i^{47}
- i^{63}
- i^{101}
- i^{141}

EXTENSION Complex Solutions of Quadratic Equations

Review of i and $\sqrt{-b}$, where $b > 0$ • The Discriminant
• Solving a Quadratic Equation

Review of i and $\sqrt{-b}$, where $b > 0$ In the **Extension Complex Numbers**, we saw that the real number system is a subset of the complex number system. The imaginary unit i , where $i = \sqrt{-1}$, is defined so that $i^2 = -1$, and a number of the form $a + bi$, where a and b are real, is called a complex number.

A square root of a negative number can be written as the product of i and a real number. Here are some examples.

$$\sqrt{-4} = i \cdot \sqrt{4} = i \cdot 2 = 2i$$

$$\sqrt{-7} = i\sqrt{7}$$

$$\sqrt{-32} = i\sqrt{32} = i\sqrt{16 \cdot 2} = 4i\sqrt{2}$$

The Discriminant In the quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

the expression under the radical symbol, $b^2 - 4ac$, is called the **discriminant**. In **Section 7.7**, we focused on quadratic equations with discriminants that were positive or zero. If the discriminant is negative, then the equation has two nonreal solutions.

Discriminant

The discriminant of $ax^2 + bx + c = 0$ is $b^2 - 4ac$. If a , b , and c are integers, then the number and type of solutions are determined as follows.

Discriminant	Number and Type of Solutions
Positive, and the square of an integer	Two rational solutions
Positive, but not the square of an integer	Two irrational solutions
Zero	One rational solution
Negative	Two nonreal solutions

EXAMPLE 1 Using the Discriminant

Show that $x^2 + x + 4 = 0$ has two nonreal complex solutions.

SOLUTION

$$\begin{aligned} b^2 - 4ac &= 1^2 - 4(1)(4) \quad \text{Here, } a = 1, b = 1, \text{ and } c = 4. \\ &= -15 \end{aligned}$$

Negative discriminant

Because $-15 < 0$, the equation has two nonreal solutions.

Solving a Quadratic Equation

EXAMPLE 2 Solving a Quadratic Equation with Nonreal Solutions

Solve $(9x + 3)(x - 1) = -8$.

SOLUTION

$$(9x + 3)(x - 1) = -8$$

$$9x^2 - 6x - 3 = -8 \quad \text{Multiply.}$$

$$9x^2 - 6x + 5 = 0 \quad \text{Add 8.}$$

From the equation $9x^2 - 6x + 5 = 0$, we identify $a = 9$, $b = -6$, and $c = 5$.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad \text{Quadratic formula}$$

$$x = \frac{-(-6) \pm \sqrt{(-6)^2 - 4(9)(5)}}{2(9)} \quad \text{Substitute.}$$

$$x = \frac{6 \pm \sqrt{-144}}{18}$$

See the Complex Numbers Extension.

$$x = \frac{6 \pm 12i}{18}$$

$$\sqrt{-144} = 12i$$

$$x = \frac{6(1 \pm 2i)}{6(3)}$$

Factor.

$$x = \frac{1 \pm 2i}{3}$$

Lowest terms

$$x = \frac{1}{3} \pm \frac{2}{3}i$$

Standard form $a + bi$ for a complex number

The solution set is $\left\{\frac{1}{3} + \frac{2}{3}i, \frac{1}{3} - \frac{2}{3}i\right\}$.



EXTENSION EXERCISES

The following equations have nonreal solutions. Use the quadratic formula and the discussion of complex numbers in this **Extension** and the **Complex Numbers Extension** to solve them.

1. $x^2 + 12 = 0$

2. $x^2 + 18 = 0$

3. $9x(x - 2) = -13$

4. $4x(x - 4) = -17$

5. $x^2 - 6x + 14 = 0$

6. $x^2 + 4x + 11 = 0$

7. $4x^2 - 4x = -7$

8. $9x^2 - 6x = -7$

9. $x(3x + 4) = -2$

10. $x(2x + 3) = -2$

EXTENSION Using Matrix Row Operations to Solve Systems

Matrix Terminology • Matrix Row Operations • Gauss-Jordan Method

NAMES MATH EDIT
 0↑cumSum(
 A: ref(
 B: rref(
 C: rowSwap(
 D: row+(
 E: *row(
 F: *row+(
)

Choices C, D, E, and F provide the user of the TI-83/84 Plus calculator a means of performing row operations on matrices.

Matrix Terminology The elimination method used to solve systems introduced in Section 8.7 can be streamlined into a systematic method by using *matrices* (singular: *matrix*). Matrices can be used to solve linear systems, and matrix methods are particularly suitable for computer solutions of large systems of equations having many unknowns.

To begin, consider a system of three equations and three unknowns such as

$$\begin{aligned} a_1x + b_1y + c_1z &= d_1 \\ a_2x + b_2y + c_2z &= d_2, \text{ written in an abbreviated form as } \begin{bmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{bmatrix} \\ a_3x + b_3y + c_3z &= d_3 \end{aligned}$$

Such a rectangular array of numbers enclosed by brackets is called a **matrix**. Each number in the array is an **element** or **entry**. The matrix above has three **rows** (horizontal) and four **columns** (vertical) of entries, and is called a 3×4 (read “3 by 4”) matrix. The constants in the last column of the matrix can be set apart from the coefficients of the variables by using a vertical line, as shown in the following **augmented matrix**.

$$\begin{array}{c} \text{Rows} \end{array} \left[\begin{array}{cc|cc} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{array} \right] \begin{array}{c} \text{Augmented matrix} \\ \text{Columns} \end{array}$$

Matrix Row Operations The rows of this augmented matrix can be treated the same as the equations of a system of equations, since the augmented matrix is actually a short form of the system. Any transformation of the matrix that will result in an equivalent system is permitted. The following **matrix row operations** produce such transformations.

Matrix Row Operations

For any real number k and any augmented matrix of a system of linear equations, the following operations will produce the matrix of an *equivalent system* — that is, another system with the same solution set.

1. **Interchange any two rows of a matrix.**
2. **Multiply the elements of a row of a matrix by the same nonzero number k .**
3. **Add a common multiple of the elements of one row to the corresponding elements of another row.**

Gauss-Jordan Method If the word “row” is replaced by “equation,” it can be seen that the three row operations also apply to a system of equations, so that a system of equations can be solved by transforming its corresponding matrix into the matrix of an equivalent, simpler system. The goal is a matrix in the form

$$\left[\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \end{array} \right] \text{ or } \left[\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \end{array} \right]$$

for systems with two or three equations respectively. On the left of the vertical bar there are ones down the diagonal from upper left to lower right and zeros elsewhere

in the matrices. When these matrices are rewritten as systems of equations, the values of the variables are known. The **Gauss-Jordan method** is a systematic way of using the matrix row operations to change the augmented matrix of a system into the form that shows its solution.

EXAMPLE 1 Solving a Linear System Using Gauss-Jordan (Two Unknowns)

Solve the linear system.

$$3x - 4y = 1$$

$$5x + 2y = 19$$

SOLUTION

The equations should all be in the same form, with the variable terms in the same order on the left, and the constant term on the right. Begin by writing the augmented matrix.

$$\left[\begin{array}{cc|c} 3 & -4 & 1 \\ 5 & 2 & 19 \end{array} \right]$$

The goal is to transform this augmented matrix into one in which the values of the variables will be easy to see. That is, since each column in the matrix represents the coefficients of one variable, the augmented matrix should be transformed so that it is of the form

$$\left[\begin{array}{cc|c} 1 & 0 & k \\ 0 & 1 & j \end{array} \right]$$

for real numbers k and j . Once the augmented matrix is in this form, the matrix can be rewritten as a linear system to get

$$x = k$$

$$y = j.$$

The necessary transformations are performed as follows. It is best to work in columns beginning in each column with the element that is to become 1. In the augmented matrix,

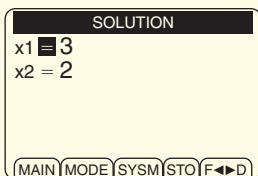
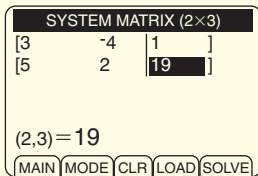
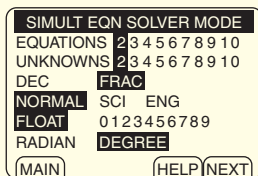
$$\left[\begin{array}{cc|c} 3 & -4 & 1 \\ 5 & 2 & 19 \end{array} \right]$$

there is a 3 in the first row, first column position. Use row operation 2, multiplying each entry in the first row by $\frac{1}{3}$ to get a 1 in this position. (This step is abbreviated as $\frac{1}{3}R1$.)

$$\left[\begin{array}{cc|c} 1 & -\frac{4}{3} & \frac{1}{3} \\ 5 & 2 & 19 \end{array} \right] \quad \frac{1}{3}R1$$

Introduce 0 in the second row, first column by multiplying each element of the first row by -5 and adding the result to the corresponding element in the second row, using row operation 3.

$$\left[\begin{array}{cc|c} 1 & -\frac{4}{3} & \frac{1}{3} \\ 0 & \frac{26}{3} & \frac{52}{3} \end{array} \right] \quad -5R1 + R2$$



The TI-84 Plus has an application that solves simultaneous equations. Compare this to **Example 1**.

Obtain 1 in the second row, second column by multiplying each element of the second row by $\frac{3}{26}$, using row operation 2.

$$\left[\begin{array}{cc|c} 1 & -\frac{4}{3} & \frac{1}{3} \\ 0 & 1 & 2 \end{array} \right] \quad \frac{3}{26} R_2$$

Finally, obtain 0 in the first row, second column by multiplying each element of the second row by $\frac{4}{3}$ and adding the result to the corresponding element in the first row.

$$\left[\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & 2 \end{array} \right] \quad \frac{4}{3} R_2 + R_1$$

This last matrix corresponds to the system

$$x = 3$$

$$y = 2,$$

that has the solution set $\{(3, 2)\}$. This solution could have been read directly from the third column of the final matrix.



A linear system with three equations is solved in a similar way. Row operations are used to get 1s down the diagonal from left to right and 0s above and below each 1.

EXAMPLE 2 Solving a System Using Gauss-Jordan (Three Unknowns)

Use the Gauss-Jordan method to solve the system.

$$x - y + 5z = -6$$

$$3x + 3y - z = 10$$

$$x + 3y + 2z = 5$$

SOLUTION

Because the system is in proper form, begin by writing the augmented matrix of the linear system.

$$\left[\begin{array}{ccc|c} 1 & -1 & 5 & -6 \\ 3 & 3 & -1 & 10 \\ 1 & 3 & 2 & 5 \end{array} \right]$$

The final matrix is to be of the form

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & m \\ 0 & 1 & 0 & n \\ 0 & 0 & 1 & p \end{array} \right],$$

where m , n , and p are real numbers. This final form of the matrix gives the system $x = m$, $y = n$, and $z = p$, so the solution set is $\{(m, n, p)\}$.

There is already a 1 in the first row, first column. Introduce a 0 in the second row of the first column by multiplying each element in the first row by -3 and adding the result to the corresponding element in the second row, using row operation 3.

$$\left[\begin{array}{ccc|c} 1 & -1 & 5 & -6 \\ 0 & 6 & -16 & 28 \\ 1 & 3 & 2 & 5 \end{array} \right] \quad -3R_1 + R_2$$

Now, to change the last element in the first column to 0, use row operation 3. Multiply each element of the first row by -1 , then add the results to the corresponding elements of the third row.

$$\left[\begin{array}{ccc|c} 1 & -1 & 5 & -6 \\ 0 & 6 & -16 & 28 \\ \mathbf{0} & \mathbf{4} & \mathbf{-3} & \mathbf{11} \end{array} \right] \quad -1R1 + R3$$

The same procedure is used to transform the second and third columns. For both of these columns, first perform the step of getting 1 in the appropriate position of each column. Do this by multiplying the elements of the row by the reciprocal of the number in that position.

$$\left[\begin{array}{ccc|c} 1 & -1 & 5 & -6 \\ \mathbf{0} & \mathbf{1} & \mathbf{-\frac{8}{3}} & \mathbf{\frac{14}{3}} \\ 0 & 4 & -3 & 11 \end{array} \right] \quad \frac{1}{6}R2$$

$$\left[\begin{array}{ccc|c} \mathbf{1} & \mathbf{0} & \mathbf{\frac{7}{3}} & \mathbf{-\frac{4}{3}} \\ 0 & 1 & -\frac{8}{3} & \frac{14}{3} \\ 0 & 4 & -3 & 11 \end{array} \right] \quad R2 + R1$$

$$\left[\begin{array}{ccc|c} 1 & 0 & \frac{7}{3} & -\frac{4}{3} \\ 0 & 1 & -\frac{8}{3} & \frac{14}{3} \\ \mathbf{0} & \mathbf{0} & \mathbf{\frac{23}{3}} & \mathbf{-\frac{23}{3}} \end{array} \right] \quad -4R2 + R3$$

$$\left[\begin{array}{ccc|c} 1 & 0 & \frac{7}{3} & -\frac{4}{3} \\ 0 & 1 & -\frac{8}{3} & -\frac{14}{3} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{-1} \end{array} \right] \quad \frac{3}{23}R3$$

$$\left[\begin{array}{ccc|c} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ 0 & 1 & -\frac{8}{3} & \frac{14}{3} \\ 0 & 0 & 1 & -1 \end{array} \right] \quad -\frac{7}{3}R3 + R1$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{2} \\ 0 & 0 & 1 & -1 \end{array} \right] \quad \frac{8}{3}R3 + R2$$

The linear system associated with this final matrix is

$$x = 1$$

$$y = 2, \text{ and the solution set is } \{(1, 2, -1)\}.$$

$$z = -1$$



SYSTEM MATRIX (3×4)				
[1	-1	5	-6]
[3	3	-1	10]
[1	3	2	5]

(3,4)=5

MAIN MODE CLR LOAD SOLVE

SOLUTION	
x1	= 1
x2	= 2
x3	= -1

MAIN MODE SYSM STO F◀▶D

Compare to **Example 2**.

EXTENSION EXERCISES

Use the Gauss-Jordan method to solve each system of equations.

1. $x + y = 5$
 $x - y = -1$

2. $x + 2y = 5$
 $2x + y = -2$

3. $x + y = -3$
 $2x - 5y = -6$

4. $3x - 2y = 4$
 $3x + y = -2$

5. $2x - 3y = 10$
 $2x + 2y = 5$

6. $4x + y = 5$
 $2x + y = 3$

7. $3x - 7y = 31$
 $2x - 4y = 18$

8. $5x - y = 14$
 $x + 8y = 11$

9. $x + y - z = 6$
 $2x - y + z = -9$
 $x - 2y + 3z = 1$

10. $x + 3y - 6z = 7$
 $2x - y + 2z = 0$
 $x + y + 2z = -1$

11. $2x - y + 3z = 0$
 $x + 2y - z = 5$
 $2y + z = 1$

12. $4x + 2y - 3z = 6$
 $x - 4y + z = -4$
 $-x + 2z = 2$

13. $-x + y = -1$
 $y - z = 6$
 $x + z = -1$

14. $x + y = 1$
 $2x - z = 0$
 $y + 2z = -2$

15. $2x - y + 4z = -1$
 $-3x + 5y - z = 5$
 $2x + 3y + 2z = 3$

16. $5x - 3y + 2z = -5$
 $2x + 2y - z = 4$
 $4x - y + z = -1$

17. $x + y - 2z = 1$
 $2x - y - 4z = -4$
 $3x - 2y + z = -7$

18. $x + 3y - 6z = -26$
 $3x + y - z = -10$
 $2x - y - 3z = -16$

Solve each problem by writing a system and solving it by the Gauss-Jordan method.

19. Company Revenue In 2009, the two American telecommunication companies with the greatest revenues were AT&T and Verizon. The two companies had combined revenues of \$221.4 billion. AT&T's revenue was \$26.6 billion more than that of Verizon. What was the revenue for each company? (Source: *Fortune* magazine.)

20. Perfume Supply A department store display features three kinds of perfume: Felice, Vivid, and Joy. There are 10 more bottles of Felice than Vivid, and 3 fewer bottles of Joy than Vivid. Each bottle of Felice costs \$8, Vivid costs \$15, and Joy costs \$32. The total value of all the perfume is \$589. How many bottles of each are there?

EXTENSION Geometric Constructions

Perpendicular Bisector • Perpendicular to a Line • Perpendicular Through a Line
• Copied Angle



Compasses may be used to:

1. Swing a circular arc with given center and radius.
2. Reproduce a given length.

(Photo courtesy of Prentice Hall.)

The Greeks did not study algebra as we do. To them geometry was the highest expression of mathematical science; their geometry was an abstract subject. Any practical application resulting from their work was nice but held no great importance.

To the Greeks, a geometrical construction also needed abstract beauty. A construction could not be polluted with such practical instruments as a ruler. The Greeks permitted only two tools in geometrical construction: compasses for drawing circles and arcs of circles, and a straightedge for drawing straight line segments. The straightedge, unlike a ruler, could have no marks on it. It was not permitted to line up points by eye.

Here are four basic constructions. Their justifications are based on the *congruence properties*.

Perpendicular Bisector Construct the perpendicular bisector of a given line segment.

Let the segment have endpoints A and B . Adjust the compasses for any radius greater than half the length of AB . Place the point of the compasses at A and draw an arc, then draw another arc of the same size at B . The line drawn through the points of intersection of these two arcs is the desired perpendicular bisector. See **Figure 23**.

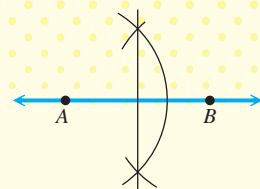


Figure 23

Perpendicular to a Line Construct a perpendicular from a point off a line to the line.

1. Let A be the point, r the line. Place the point of the compasses at A and draw an arc, cutting r in two points.
2. Swing arcs of equal radius from each of the two points on r which were constructed in (1). The line drawn through the intersection of the two arcs and point A is perpendicular to r . See **Figure 24**.

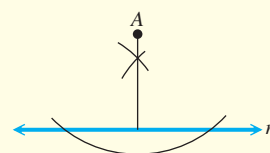
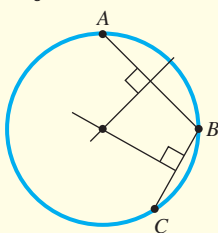


Figure 24

In his first effort as a director, Mel Gibson starred in the 1993 movie *The Man Without a Face*. As disfigured former teacher Justin McLeod, he tutors teenager Chuck Norstadt (portrayed by Nick Stahl). McLeod explains to Norstadt how to find the center of a circle using any three points on the circle as he sketches the diagram on a windowpane. His explanation is based on the fact that the **perpendicular bisector** of any chord of a circle passes through the center of the circle. See the figure.



Perpendicular Through a Line Construct a perpendicular to a line at some given point on the line.

1. Let r be the line and A the point. Using any convenient radius on the compasses, place the point of the compasses at A and swing arcs that intersect r , as in **Figure 25**.



Figure 25

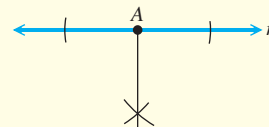


Figure 26

2. Increase the radius of the compasses, place the point of the compasses on the points obtained in (1) and draw arcs. A line through A and the intersection of the two arcs is perpendicular to r . See **Figure 26**.

There were three constructions that the Greeks were not able to accomplish with **Euclidean tools**, specifically the compasses and unmarked straightedge.

Now known as the **three famous problems of antiquity**, they are:

1. To trisect an arbitrary angle;
2. To construct the length of the edge of a cube having twice the volume of a given cube;
3. To construct a square having the same area as that of a given circle.

In the nineteenth century it was discovered that these constructions are, in fact, impossible to accomplish with Euclidean tools.

Copied Angle Copy an angle.

1. In order to copy an angle ABC on line r , place the point of the compasses at B and draw an arc. Then place the point of the compasses on r' at some point P and draw the same arc, as in **Figure 27**.

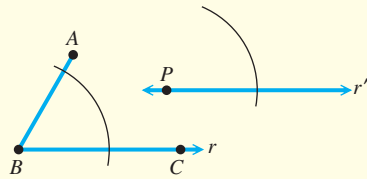


Figure 27

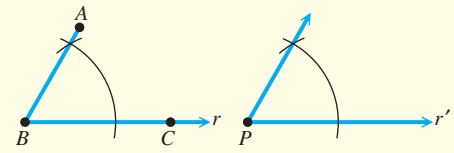


Figure 28

2. Measure, with your compasses, the distance between the points where the arc intersects the angle, and transfer this distance, as shown in **Figure 28**. Use a straightedge to join P to the point of intersection. The angle is now copied.

There are other basic constructions that can be found in books on plane geometry.

EXTENSION EXERCISES

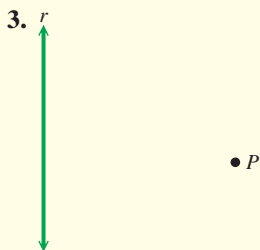
In Exercises 1 and 2, construct the perpendicular bisector of segment PQ .



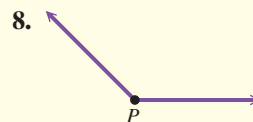
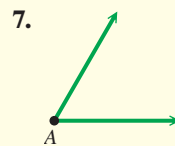
In Exercises 5 and 6, construct a perpendicular through the line r at P .



In Exercises 3 and 4, construct a perpendicular from P to the line r .



In Exercises 7 and 8, copy the given angle.



9. It is impossible to trisect the general angle using only Euclidean tools. Investigate this fact, and write a short report on it. Include in your report information on the construction tool called a *tomahawk*.

EXTENSION Regression and Correlation

Linear Regression • Correlation

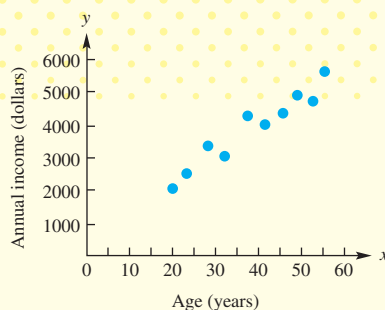
Table 18 Age vs. Income		
Resident	Age	Annual Income
A	19	2150
B	23	2550
C	27	3250
D	31	3150
E	36	4250
F	40	4200
G	44	4350
H	49	5000
I	52	4950
J	54	5650

Linear Regression One very important branch of inferential statistics, called **regression analysis**, is used to compare quantities or variables, to discover relationships that exist between them, and to formulate those relationships in useful ways.

Suppose a sociologist gathers data on a few (say ten) of the residents of a small village in a remote region in order to get an idea of how annual income (in dollars) relates to age in that village. The data are shown in **Table 18**.

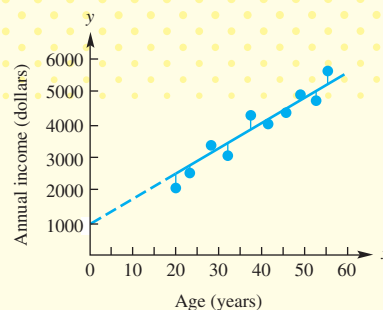
The first step in analyzing these data is to graph the results, as shown in the **scatter diagram** of **Figure 24**. (Graphing calculators will plot scatter diagrams.)

Once a scatter diagram has been produced, we can draw a curve that best fits the pattern exhibited by the sample data points. This curve can have any one of many characteristic shapes, depending on how the quantities involved are related. The best-fitting curve for the sample points is called an **estimated regression curve**. If, as in the present discussion, the points in the scatter diagram seem to lie approximately along a straight line, the relation is assumed to be linear, and the line that best fits the data points is called the **estimated regression line**.



Scatter diagram

Figure 24



A tentative estimated regression line

Figure 25

If we let x denote age and y denote income in the data of **Table 18** and assume that the best-fitting curve is a line, then the equation of that line will take the form

$$y = ax + b,$$

where a is the slope of the line and b is the y -coordinate of the y -intercept (the y -value at which the line, if extended, would intersect the y -axis).

To completely identify the estimated regression line, we must find the values of the **regression coefficients** a and b , which requires some calculation. In **Figure 25**, a tentative line has been drawn through the scatter diagram.

For each x -value in the data set, the corresponding y -value usually differs from the value it would have if the data point were exactly on the line. These differences are shown in the figure by vertical segments. Choosing another line would make some of these differences greater and some lesser. The most common procedure is to choose the line where the sum of the squares of all these differences is minimized. This is called the **method of least squares**, and the resulting line is called the **least squares line**.

In the equation of the least squares line, the variable y' can be used to distinguish the *predicted* values (which would give points on the least squares line) from the *observed* values y (those occurring in the data set).

The least squares criterion mentioned above leads to specific values of a and b . We shall not give the details, which involve differential calculus, but the results are given here. (Σ — the Greek letter *sigma* — represents summation just as in earlier sections.)

Regression Coefficient Formulas

The **least squares line** $y' = ax + b$ that provides the best fit to the data points $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ has coefficient values as follows.

$$a = \frac{n(\sum xy) - (\sum x)(\sum y)}{n(\sum x^2) - (\sum x)^2} \quad b = \frac{\sum y - a(\sum x)}{n}$$

EXAMPLE 1 Computing and Graphing a Least Squares Line

Find the equation of the least squares line for the age and income data given in **Table 18**. Graph the line.

SOLUTION

Start with the two columns on the left in **Table 19** (which just repeat the original data). Then find the products $x \cdot y$, and the squares x^2 .

Table 19 Age and Income Calculations			
x	y	$x \cdot y$	x^2
19	2150	40,850	361
23	2550	58,650	529
27	3250	87,750	729
31	3150	97,650	961
36	4250	153,000	1296
40	4200	168,000	1600
44	4350	191,400	1936
49	5000	245,000	2401
52	4950	257,400	2704
54	5650	305,100	2916
Sums: 375	39,500	1,604,800	15,433

Francis Galton (1822–1911) learned to read at age three, was interested in mathematics and machines, but was an indifferent mathematics student at Trinity College, Cambridge. He became interested in researching methods of predicting weather. It was during this research that Galton developed early intuitive notions of **correlation** and **regression** and posed the problem of multiple regression.

Galton's key statistical work is *Natural Inheritance*. In it, he set forth his ideas on regression and correlation. He discovered the correlation coefficient while pondering Alphonse Bertillon's scheme for classifying criminals by physical characteristics. It was a major contribution to statistical method.

From the table, $\sum x = 375$, $\sum y = 39,500$, $\sum xy = 1,604,800$, and $\sum x^2 = 15,433$. There are 10 pairs of values, so $n = 10$. Now find a with the formula given above.

$$a = \frac{10(1,604,800) - 375(39,500)}{10(15,433) - (375)^2} = \frac{1,235,500}{13,705} \approx 90.15$$

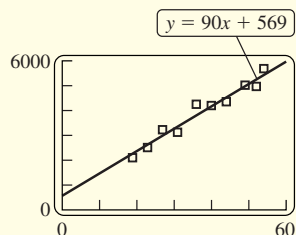
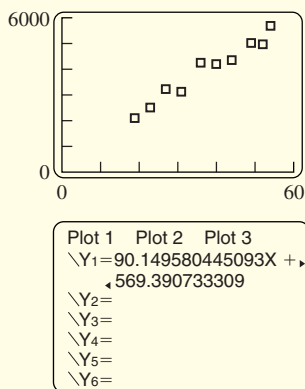
Finally, use this value of a to find b .

$$b = \frac{39,500 - 90.15(375)}{10} \approx 569.4$$

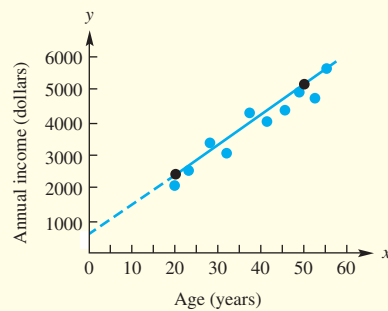
The equation of the least squares line can now be written.

$$y' = 90x + 569 \quad \text{Coefficients are rounded.}$$

Letting $x = 20$ in this equation gives $y' = 2369$, and $x = 50$ implies $y' = 5069$. The two points $(20, 2369)$ and $(50, 5069)$ are used to graph the regression line in **Figure 26** on the next page. Notice that the intercept coordinates $(0, 569)$ also fit the extended line.



The information in **Figure 26** and the accompanying discussion is supported in these screens.



Least squares line

Figure 26

A computer or a scientific, statistical, or graphing calculator is recommended for finding regression coefficients. Tedious calculations, such as in **Example 1**, can be avoided and the regression line produced automatically.

EXAMPLE 2 Predicting from a Least Squares Line

Use the result of **Example 1** to predict the income of a village resident who is 35 years old.

SOLUTION

$$y' = 90x + 569 \quad \text{Equation from Example 1}$$

$$y' = 90(35) + 569 \quad \text{Let } x = 35.$$

$$y' = 3719$$

Based on the given data, a 35-year-old will make about \$3719 per year.

Correlation Once an equation for the line of best fit (the least squares line) has been found, it is reasonable to ask, “Just how good is this line for predictive purposes?” If the points already observed fit the line quite closely, then future pairs of scores can be expected to do so. If the points are widely scattered about even the “best-fitting” line, then predictions are not likely to be accurate.

In general, the closer the *sample* data points lie to the least squares line, the more likely it is that the entire *population* of (x, y) points really do form a line, that is, that x and y really are related linearly. Also, the better the fit, the more confidence we can have that our least squares line (based on the sample) is a good estimator of the true population line.

One common measure of the strength of the linear relationship in the sample is called the **sample correlation coefficient**, denoted r . It is calculated from the sample data according to the following formula.

Sample Correlation Coefficient Formula

In linear regression, the strength of the linear relationship is measured by the correlation coefficient r , calculated as follows.

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{n(\sum x^2) - (\sum x)^2} \cdot \sqrt{n(\sum y^2) - (\sum y)^2}}$$

The value of r is always between -1 and 1 , or perhaps equal to -1 or 1 . The degree of fit (correlation) can be described in general terms, according to the value of r , as follows.

Degree of Fit of an Estimated Regression Line to Sample Data Points

- Perfect fit: $r = 1$ or $r = -1$
- Strong fit: r close (but not equal) to 1 or -1
- Moderate fit: r not close to 0 , and not close to 1 or -1
- Weak fit: r equal, or nearly equal, to 0

The sign (plus or minus) of r determines the type of linear relationship, if any, between the variables x and y .

Direct and Inverse Linear Relationships

- If $r > 0$, the regression line has positive slope. The relationship between x and y is **direct**—as x increases, y also increases.
- If $r < 0$, the regression line has negative slope. The relationship between x and y is **inverse**—as x increases, y decreases.
- If $r = 0$, no linear relationship between x and y is indicated.

EXAMPLE 3 Finding a Correlation Coefficient

Find r for the age and income data of **Table 19**.

SOLUTION

Almost all values needed to find r were computed in **Example 1**.

$$n = 10 \quad \Sigma x = 375 \quad \Sigma y = 39,500 \quad \Sigma xy = 1,604,800 \quad \Sigma x^2 = 15,433$$

The only missing value is Σy^2 . Squaring each y in the original data and adding the squares gives

$$\Sigma y^2 = 167,660,000.$$

Now use the formula to find that $r = 0.98$ (to two decimal places). This value of r , very close to 1 , shows that age and income in this village are highly correlated. (The fit of the estimated regression line is strong.) The fact that r is positive indicates that the linear relationship is direct; as age increases, income also increases. ■■■

EXAMPLE 4 Analyzing the Aging Trend in the U.S. Population

The World Almanac and Book of Facts 2010 (page 622) reported the following U.S. Census Bureau data concerning the aging U.S. population over the last century. Let x represent time, in decades, from 1910, so $x = 0$ in 1910, $x = 1$ in 1920, $x = 2$ in 1930, and so on. Let y represent percent 65 and over in the population. Based on the data table, carry out the following.

Year	1910	1920	1930	1940	1950	1960	1970	1980	1990	2000	2010
Percent 65 and over	4.3	4.7	5.4	6.8	8.1	9.2	9.8	11.3	12.5	12.4	13.0

LinReg
 $y = ax + b$
 $a = 90.14958045$
 $b = 569.3907333$
 $r^2 = .9572823948$
 $r = .9784080922$

The slope a and y -intercept b of the regression equation, along with r^2 and r , are given. Compare with **Examples 1 and 3**.

Let x represent time, in decades, from 1910, so $x = 0$ in 1910, $x = 1$ in 1920, $x = 2$ in 1930, and so on. Let y represent percent 65 and over in the population. Based on the data table, carry out the following.

- Plot a scatter diagram.
- Compute and graph the least squares regression line.
- Compute the correlation coefficient.
- Use the regression line to predict the percent 65 and over in 2050, and discuss the validity of the prediction.

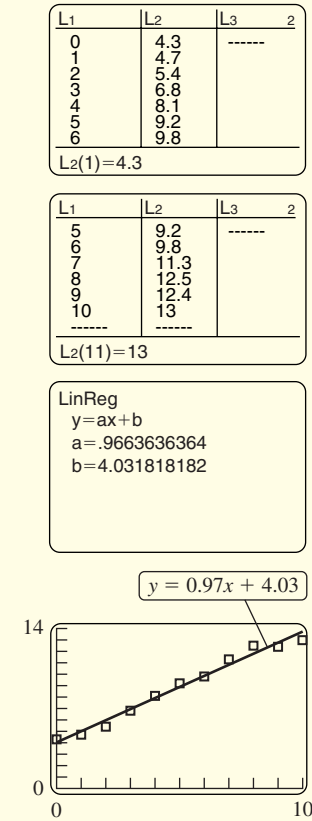
SOLUTION

- The data points are plotted in **Figure 27**.

- We entered the x - and y -values into lists L1 and L2, respectively, in a calculator to obtain the equation of the least squares regression line.

$$y' = 0.97x + 4.03 \quad \text{Coefficients are rounded.}$$

This line is shown in **Figure 27** as a dashed line.



These screens support **Example 4(b)**.

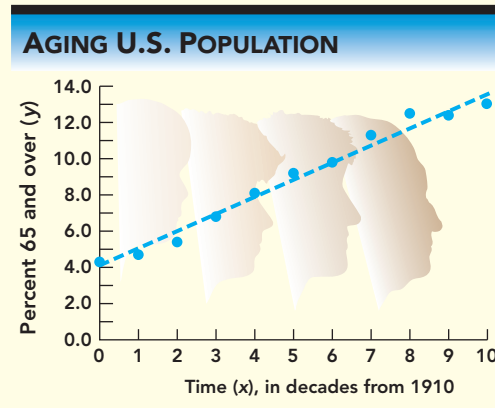


Figure 27

- $\Sigma x = 55$, $\Sigma x^2 = 385$, $n = 11$, $\Sigma y = 97.5$,

All values are from the calculator, using two-variable statistics.

$$\Sigma y^2 = 968.97, \quad \Sigma (xy) = 593.8$$

$$r = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{n(\Sigma x^2) - (\Sigma x)^2} \cdot \sqrt{n(\Sigma y^2) - (\Sigma y)^2}} \quad \text{Correlation coefficient formula}$$

$$= \frac{11 \cdot 593.8 - 55 \cdot 97.5}{\sqrt{11 \cdot 385 - 55^2} \cdot \sqrt{11 \cdot 968.97 - 97.5^2}}$$

$$= 0.990211 \dots$$

$$r \approx 0.99$$

- $y' = 0.97x + 4.03$ Estimated regression line
 $= 0.97 \cdot 14 + 4.03$ The year 2050 corresponds to $x = 14$.
 $y \approx 17.6$ 17.61 has been rounded here.

Although the correlation was strong ($r \approx 0.99$) for the data points we had, it is risky to extrapolate a regression line too far out. There may be factors (such as declining numbers of baby boomers in the population) that may slow the aging phenomenon. (Incidentally, the Census Bureau projects 20.2% in 2050.)

EXTENSION EXERCISES

Correlating Fertilizer and Corn Ear Size In a study to determine the linear relationship between the length (in decimeters) of an ear of corn (y) and the amount (in tons per acre) of fertilizer used (x), the following values were determined.

$$\begin{aligned} n &= 10 & \Sigma xy &= 75 \\ \Sigma x &= 30 & \Sigma x^2 &= 100 \\ \Sigma y &= 24 & \Sigma y^2 &= 80 \end{aligned}$$

- Find an equation for the least squares line.
- Find the correlation coefficient.
- If 3 tons per acre of fertilizer are used, what length (in decimeters) would the regression equation predict for an ear of corn?

Correlating Celsius and Fahrenheit Temperatures In an experiment to determine the linear relationship between temperatures on the Celsius scale (y) and on the Fahrenheit scale (x), a student got the following results.

$$\begin{aligned} n &= 5 & \Sigma xy &= 28,050 \\ \Sigma x &= 376 & \Sigma x^2 &= 62,522 \\ \Sigma y &= 120 & \Sigma y^2 &= 13,450 \end{aligned}$$

- Find an equation for the least squares line.
- Find the reading on the Celsius scale that corresponds to a reading of 120° Fahrenheit, using the equation of **Exercise 4**.
- Find the correlation coefficient.

Correlating Heights and Weights of Adult Men A sample of 10 adult men gave the following data on their heights and weights.

Height (inches) (x)	62	62	63	65	66
Weight (pounds) (y)	120	140	130	150	142
Height (inches) (x)	67	68	68	70	72
Weight (pounds) (y)	130	135	175	149	168

- Find the equation of the least squares line.
- Using the results of **Exercise 7**, predict the weight of a man whose height is 60 inches.
- What would be the predicted weight of a man whose height is 70 inches?
- Compute the correlation coefficient.

Correlating Reading Ability and IQs The table below gives reading ability scores and IQs for a group of 10 individuals.

Reading (x)	83	76	75	85	74
IQ (y)	120	104	98	115	87
Reading (x)	90	75	78	95	80
IQ (y)	127	90	110	134	119

- Plot a scatter diagram with reading on the horizontal axis.
- Find the equation of a regression line.
- Use your regression line equation to estimate the IQ of a person with a reading score of 65.

Correlating Yearly Sales of a Company Sales, in thousands of dollars, of a certain company are shown here.

Year (x)	0	1	2	3	4	5
Sales (y)	48	59	66	75	80	90

- Find the equation of the least squares line.
- Find the correlation coefficient.
- If the linear trend displayed by this data were to continue beyond year 5, what sales amount would you predict in year 7?

Comparing the Ages of Dogs and Humans It often is said that a dog's age can be multiplied by 7 to obtain the equivalent human age. A more accurate correspondence (through the first 14 years) is shown in this table from *The Old Farmer's Almanac, 2000 edition, page 180*.

Dog age (x)	$\frac{1}{2}$	1	2	3	4	5	6	7
Equivalent human age (y)	10	15	24	28	32	36	40	44
Dog age (x)	8	9	10	11	12	13	14	
Equivalent human age (y)	48	52	56	60	64	68	70.5	


- Plot a scatter diagram for the given data.
- Find the equation of the regression line, and graph the line on the scatter diagram of **Exercise 17**.
- Describe where the data points show the most pronounced departure from the regression line, and explain why this might be so.

20. Compute the correlation coefficient.

Statistics on the Westward Population Movement The data show the increase in the percentage of U.S. population in the West since about the time of the California Gold Rush.

Census Year	Time, in Decades from 1850 (x)	Percentage in West (y)
1850	0	0.8%
1870	2	2.6
1890	4	5.0
1910	6	7.7
1930	8	10.0
1950	10	13.3
1970	12	17.1
1990	14	21.2

Source: *The World Almanac and Book of Facts 2000*.

21. Taking x and y as indicated in the table, find the equation of the regression line.
22. Compute the correlation coefficient.
23. Describe the degree of correlation (for example, as strong, moderate, or weak).
-  24. Would you expect the linear trend apparent in the table to persist into the mid 21st century? Why or why not?

Comparing State Populations with Governors' Salaries The table shows the ten most populous states (as of 2008) and the salaries of their governors (as of September 2009).

Rank	State	Population, in Millions (x)	Governor's Salary, in Thousands of Dollars (y)
1	California	37	174
2	Texas	24	150
3	New York	19	179
4	Florida	18	130
5	Illinois	13	177
6	Pennsylvania	12	175
7	Ohio	11	142
8	Michigan	10	177
9	Georgia	10	139
10	North Carolina	9	140

Source: *The World Almanac and Book of Facts 2010*.

25. Find the equation of the estimated regression line.
26. Compute the correlation coefficient.
27. Describe the degree of correlation (for example, as strong, moderate, or weak).
28. What governor's salary would this linear model predict for a state with a population of 15 million citizens?

EXTENSION Ponzi Schemes and Other Investment Frauds*

Geometric Sequences • Pyramid Schemes • Ponzi Schemes

Geometric Sequences In a **geometric sequence**, each term after the first is generated by multiplying the previous term by the **common ratio**, a number remaining constant throughout the sequence. For example, a geometric sequence with first term 3 and common ratio 2 starts out as follows:

$$3, 6, 12, 24, 48, 96, \dots$$

In general, if the first term is denoted a , the common ratio is denoted r , and there are n terms altogether, then the complete sequence is

$$a, ar, ar^2, ar^3, \dots, ar^{n-1}.$$

(Verify by inductive reasoning that the n th term really is ar^{n-1} .)

The sum of all n terms of the geometric sequence above can be written

$$S = a + ar + ar^2 + \dots + ar^{n-2} + ar^{n-1}.$$

Multiply both sides of this equation by r :

$$Sr = ar + ar^2 + ar^3 + \dots + ar^{n-1} + ar^n.$$

Now position these two equations, one below the other, and subtract as follows.

$$\begin{array}{r} S = a + ar + ar^2 + \dots + ar^{n-2} + ar^{n-1} \\ Sr = ar + ar^2 + ar^3 + \dots + ar^{n-1} + ar^n \\ \hline S - Sr = (a - ar) + (ar - ar^2) + (ar^2 - ar^3) + \dots + (ar^{n-2} - ar^{n-1}) + (ar^{n-1} - ar^n) \end{array}$$

Now we can rearrange and regroup the terms on the right to obtain the following.

$$\begin{aligned} S - Sr &= a + (ar - ar) + (ar^2 - ar^2) + \dots + (ar^{n-1} - ar^{n-1}) - ar^n \\ &= a + 0 + 0 + \dots + 0 - ar^n \end{aligned}$$

Notice that all terms on the right, except a and $-ar^n$, were arranged in pairs to cancel out. So we get the following.

$$\begin{aligned} S - Sr &= a - ar^n \\ S(1 - r) &= a(1 - r^n) && \text{Factor both sides.} \\ S &= \frac{a(1 - r^n)}{1 - r} && \text{Solve for the sum } S. \end{aligned}$$

The Sum of a Geometric Sequence

If a geometric sequence has first term a and common ratio r , and has n terms altogether, then the sum of all n terms is calculated as follows.

$$S = \frac{a(1 - r^n)}{1 - r}$$

The ability to recognize a geometric sequence and to sum its terms is very helpful in many applications, including detecting investment fraud.

Pyramid Schemes Most everyone has been invited, through email or otherwise, to pass on some message to two (or more) other people. Sometimes it is an innocent “chain letter.” But if it involves sending money to someone, it is likely a **pyramid scheme**.

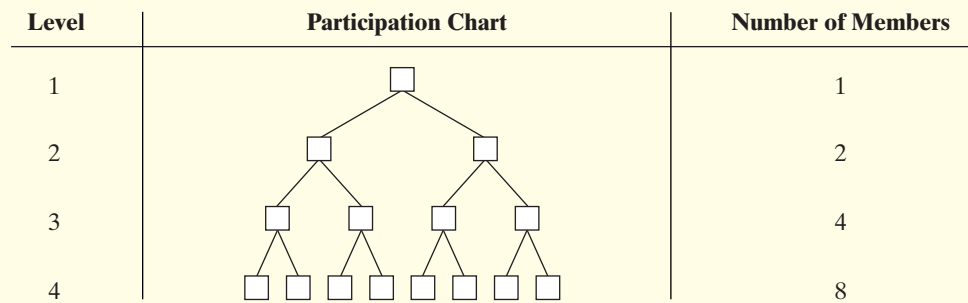
*Sources: www.usatoday.com, www.moneymorning.com, www.nytimes.com, www.wikipedia.org

EXAMPLE 1 Analyzing Payoffs in a Pyramid Scheme

You receive a letter with a list of three names, along with the following instructions.

1. Send \$1 to the top name on the list.
2. Remove that name and move the other two names up on the list.
3. Add your own name at the bottom of the list.
4. Send the same letter, with the new list, to two other people.

Suppose you decide to participate (become a member), both of your two recruits also participate, all of their four recruits participate, and all of their eight recruits participate. We call this the “each one recruits two” model. (It is also known, classically, as the 8-ball model.) You and the next three levels of participation are illustrated in **Figure 1**.



Participation chart for an 8-ball pyramid scheme

Figure 1

- (a) With you and all your downstream recruits, how many members are there?
- (b) How much money will you receive?
- (c) What is your profit?

SOLUTION

(a) $1 + 2 + 4 + 8 = 15$

(b) You receive \$1 from each level-4 member, for a total of \$8.

Income Cost
↓ ↓

(c) Profit = \$8 − \$1 = \$7 (minus two envelopes and two postage stamps) ■■■

Observe, from **Figure 1** of **Example 1**, that, beginning with one member at level 1, the number of members in a given level is double the number of members in the previous level.

EXAMPLE 2 Finding the Number of Members in a Pyramid Scheme

For each of the following numbers of levels, find the total number of members, from level 1 up to and including the given level. Use inductive reasoning in part (c).

- (a) 4 (b) 7 (c) N

SOLUTION

(a) $1 + 2 + 4 + 8 = 15$ (or, $2^4 - 1$)

(b) $1 + 2 + 4 + 8 + 16 + 32 + 64 = 127$ (or, $2^7 - 1$)

(c) Assuming the pattern observed in parts (a) and (b) holds, the total number of members from level 1 through level N , inclusive, would be

$$2^N - 1.$$



The expression, $2^N - 1$, of **Example 2(c)** was derived inductively, but can also be deduced using the formula for the sum of a geometric sequence given earlier.

EXAMPLE 3 Deducing the Number of Members in a Pyramid Scheme

Use deductive reasoning to *prove* that $2^N - 1$ is the total number of members in an “each one recruits two” pyramid with N levels.

SOLUTION

The number of members in the N levels are 1, 2, 4, 8, . . . , and 2^{N-1} . Their sum is the sum of a geometric sequence with

first term $a = 1$, common ratio $r = 2$, number of terms $n = N$.

So the sum is found as follows.

$$\begin{aligned} S &= \frac{a(1 - r^n)}{1 - r} && \text{Sum formula} \\ &= \frac{1(1 - 2^N)}{1 - 2} && \text{Substitute } a = 1, r = 2, n = N. \\ &= \frac{2^N - 1}{2 - 1} && \text{Multiply numerator and denominator by } -1. \\ &= 2^N - 1 && \text{Simplify.} \end{aligned}$$



Table 11 summarizes the various values involved as the pyramid builds downward.

Table 11 The Numbers in an “Each One Recruits Two” Pyramid Scheme		
Level Number n	Number of Members in Level n	Total Number of Members in all Levels Up To and Including Level n
1	$1 = 2^{1-1}$	$1 = 2^1 - 1$
2	$2 = 2^{2-1}$	$1 + 2 = 3 = 2^2 - 1$
3	$4 = 2^{3-1}$	$1 + 2 + 4 = 7 = 2^3 - 1$
4	$8 = 2^{4-1}$	$1 + 2 + 4 + 8 = 15 = 2^4 - 1$
5	$16 = 2^{5-1}$	$1 + 2 + 4 + 8 + 16 = 31 = 2^5 - 1$
.	.	.
.	.	.
.	.	.
N	2^{N-1}	$1 + 2 + 4 + 8 + 16 + \dots + 2^{N-1} = 2^N - 1$

The fact that a **pyramid scheme** profits relatively few at the expense of many, most of whom don't really understand how it works, is part of why these schemes are illegal in the United States (and many other countries). If participants are provided goods or services comparable in value to their "entry fee," then the combination of promotion (recruiting) and selling (goods or services) can become (technically) a legal multi-level marketing (MLM) plan. But there is a fine line between legitimate business and fraud. The legal distinction rests on whether the recruitment exists to promote the product or the product exists to promote the recruitment.

The pyramid must keep building downward indefinitely if all the members are to receive their profit. But a pyramid with, say, 20 levels requires

$$2^{20} - 1 = 1,048,575 \text{ members.}$$

And just 33 levels would involve

$$2^{33} - 1 = 8,589,934,591 \text{ members,}$$

which exceeds the population of the world. Therefore, every pyramid scheme must eventually fail, and most likely long before achieving 33 levels. And when it fails, the members in the last three levels will not get paid. This means that if failure occurs after N levels, then the number of members who lose their money is

$$2^{N-1} + 2^{N-2} + 2^{N-3}.$$

We can now express the fraction of all participants who will lose money as follows.

$$\begin{aligned} \text{Fraction who lose} &= \frac{2^{N-1} + 2^{N-2} + 2^{N-3}}{2^N - 1} && \leftarrow \begin{array}{l} \text{Number who lose} \\ \text{Number who participate} \end{array} \\ &= \frac{2^{N-3}(2^2 + 2 + 1)}{2^N - 1} && \text{Factor } 2^{N-3} \text{ from numerator.} \\ &= \frac{2^{N-3}(7)}{2^N - 1} && \text{Add.} \end{aligned}$$

Now deleting the -1 from the denominator makes the denominator (slightly) greater, hence the overall fraction lesser. So we can state the following.

$$\begin{aligned} \text{Fraction who lose} &> \frac{2^{N-3}(7)}{2^N} \\ &= \frac{7}{2^{N-(N-3)}} && \text{Apply rule of exponents.} \\ &= \frac{7}{2^3} && \text{Simplify exponent.} \\ &= \frac{7}{8} && \text{Simplify.} \end{aligned}$$

Charles Ponzi, like many other scheme operators who followed him, possessed personal attributes, including charm and salesmanship, that allowed him to accumulate much more than what was required just to pay out the profits demanded. As he seemed to be making good on his promises, most investors left both principal and profit to increase in the plan. On some days, he had thousands of zealous investors lined up to give him their money.

It is important, for the success of a Ponzi scheme, that the illusion of successful investment returns be maintained early on to build confidence and attract an ever-growing number of investors. And it helps if the true details of the operation are obscure and difficult or impossible to actually verify.

No matter how many levels succeed, everyone in the last three levels loses, and these are more than $\frac{7}{8}$ of all participants.

Ponzi Schemes Pyramid schemes are relatively straightforward, though promoters tend to avoid the use of terms like "pyramid" and "scheme." **Ponzi schemes**, on the other hand, come in many varieties and usually involve financial instruments (like "derivatives") and terms (like "alternative asset classes") that can confuse even experienced investors. These scams always pretend to offer real investment returns of one kind or another, but in fact an investor's "returns" come only from his own money or from the deposits of later investors.

The name comes from the years following World War I, when an Italian immigrant, Charles Ponzi, realized that non-uniform international currency exchange rates and other factors made it possible, theoretically, to profit by buying postal reply coupons in Italy and exchanging them for U.S. stamps. There was a money-making potential in this, but over time, Ponzi solicited and received far more deposits ("investments") than could be placed in that market. His operation, mostly in the New England area, drew in more and more participants as he returned profits to early investors out of the deposits of later investors.

EXAMPLE 4**Finding the Minimum Number of Investors Needed to Support a Ponzi Scheme**

Ponzi promised investors a 50% profit within 45 days or a 100% profit within 90 days. Assuming that he started the year with one investor, who put in \$1000, and that all investors always withdrew their 90-day profit and left their principal with Ponzi, how many investors would he need within a year?

SOLUTION

Consider the absolute minimum number of investors required at the end of each quarter (although this certainly was not Ponzi's objective).

- After one quarter (90 days) the single investor's \$1000 could be paid back to him as his quarterly profit. So at that point no new investors are necessary.
- At the end of the second quarter, the investor wants another \$1000 profit, and no money is available without an additional investor. So one investor must be added. His deposit can be used to pay the original investor.
- At the end of the third quarter, there are two investors, and no money. Two additional investors must be recruited to pay profits to the two previous investors.
- At the end of the fourth quarter (one year), four investors expect quarterly profit, so four new investors must be recruited.

Just to pay out profits, Ponzi would need to double his number of investors at the end of each quarter starting with the second. By the end of the year, 1 has doubled to 2, 2 to 4, and 4 to 8. He must end the year with 8 investors. Nothing is left for Ponzi. And if anyone wanted their principal back, he would be in trouble. ■■■

EXAMPLE 5**Analyzing Cash Flow in a Ponzi Scheme**

Suppose that investors are promised 100% profit per quarter. At the beginning of each quarter (90 days), 1000 investors contribute \$1000 each, and all monies stay in until the end of the year. There are then four categories of investors.

1. those who have been in for 4 quarters
2. those who have been in for 3 quarters
3. those who have been in for 2 quarters
4. those who have been in for 1 quarter

At the end of the year, 10% of those in each category take out their profits, but leave their principal. What amount does that leave with the operator?

SOLUTION

The amount taken in during the year is $4000 \cdot \$1000 = \$4,000,000$. At the end of the year, the supposed profits would be: \$4000 for each category 1 investor, \$3000 for each category 2 investor, \$2000 for each category 3 investor, and \$1000 for each category 4 investor. Ten percent of each category take out their profits, and 10% of 1000 is 100, so the payout would then be

$$\begin{array}{ccccccc}
 \text{Category 1} & & \text{Category 2} & & \text{Category 3} & & \text{Category 4} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 100 \cdot \$4000 & + & 100 \cdot \$3000 & + & 100 \cdot \$2000 & + & 100 \cdot \$1000 = \$1,000,000.
 \end{array}$$

The amount the operator retains is

$$\$4,000,000 - \$1,000,000 = \$3,000,000. \quad \blacksquare$$

The 2010 book *No One Would Listen*, by Harry Markopolos, describes the longest running and largest Ponzi scheme ever revealed, as well as the futile efforts made by Markopolos, over a decade, to convince governmental regulators to take action against its operator, Bernard Madoff. (See **Exercises 23–25**.) Extensive resources, for the general reader and for classroom use, are available at www.noonewouldlisten.com.

EXTENSION EXERCISES

Analyzing an “Each One Recruits Three” Pyramid Scheme For Exercises 1–11, consider a pyramid scheme just like in **Example 1**, except that “each one recruits three,” rather than two. (Work these all, in order.)

- Draw a chart like in **Example 1** showing the first four levels.
- How many members are in each of the following levels?
(a) 1 (b) 2 (c) 3 (d) 4
- If the chart is extended, in general how many members are in level N ?
- If you are the top person in the chart, and each person’s entry fee is \$1, how much money will you receive?
- What will your profit be?
- What is the total number of members, from level 1 through each of the following levels, inclusive?
(a) 1 (b) 2
(c) 3 (d) 4
(e) 5 (f) 6
- Fill in the blanks in the following statements. The total number of members in levels 1 through N , inclusive, is $1 + 3 + 9 + \dots + \underline{\hspace{2cm}}$. This is the sum of a $\underline{\hspace{2cm}}$ sequence with $a = \underline{\hspace{1cm}}$, $r = \underline{\hspace{1cm}}$, and $n = \underline{\hspace{1cm}}$. So the total number of members is $\underline{\hspace{2cm}}$.
- If the pyramid fails after level N , how many members will lose?
- Suppose the scheme runs through level 6 and then fails. How many members lose?
- Under the conditions of **Exercise 9**, what fraction of the members lose?
- In an “each one recruits two” pyramid scheme, it was shown that more than $\frac{7}{8}$ of all members will lose. Use a similar analysis to characterize the fraction who will lose in an “each one recruits three” scheme.

- Suppose you enter an “each one recruits two” pyramid scheme (at level 1), paying your \$1 entry fee. If x denotes the number of level-4 recruits that eventually send you \$1, then x is a random variable that can take on any of the values 0, 1, 2, 3, 4, 5, 6, 7, or 8. If the probability that any given person invited to join actually will join is $\frac{1}{2}$, then, using binomial probabilities gives the following probability distribution for x .

x	$P(x)$
0	0.34361
1	0.39270
2	0.19635
3	0.05610
4	0.01002
5	0.00114
6	0.00008
7	0.00000
8	0.00000

Find each of the following.

- the sum of these probability values
- your expected income


- In **Exercise 12**, what is your expected profit?
- If you were initiating a pyramid scheme, what would be the advantages and disadvantages of “each one recruits three” rather than two?
- In a pyramid scheme, even if you and your three levels of recruits are embedded in a much larger chart, with multiple levels above you and many more below you, it is still only your four levels that affect your cost and income. Explain why this is so.
- In an “each one recruits two” pyramid scheme, more than $\frac{7}{8}$ of all members will lose. What is the *greatest* fraction that could lose, and how could it happen?
- Discuss places you have encountered “chain letters” or pyramid schemes with promises of money rewards for entering.
- A number of other types of frauds have surfaced over the years. (Someone always has a new angle.) Research and write a report on “matrix schemes.”

Finding the Required Number of Investors in a Ponzi Scheme Refer to **Example 4** for Exercises 19 and 20.

19. How many investors would be required by the end of two years with the same promised return of 100% per 90 days?
20. If the year began with 1000 investors, how many would be required at the end of each time period?
(a) one year (b) two years (c) three years


Exploring Cash Flow in a Ponzi Scheme Refer to **Example 5** for Exercises 21 and 22.


21. Suppose that at the end of the year, those 10% of investors actually invest another \$1000 rather than taking out profit. Now what amount stays with the operator going into the second year?


- 
22. Explain what factors may have convinced investors to put in more money and not take out profit.

Bernie Made Off with Billions. As of mid 2010, the largest Ponzi scheme in history was operated by Bernard Madoff, a New York financier and former chairman of the NASDAQ Stock Market. When he was arrested in December of 2008, Mr. Madoff had swindled investors, including charities, foundations, large hedge funds, and funds of funds, as well as individuals, out of some \$21 billion. He claimed to be trading in Standard & Poor's 500 Index options, but no one could tell what his fund actually held because he sold out of each option before reporting became mandatory.

23. Assume that Charles Ponzi bilked his investors out of \$4 million in 1920. If inflation averaged 3% from 1920 to 2008, compare the magnitudes of the Ponzi and Madoff scams in comparable dollars.

- 
24. Speculate as to whether Bernard Madoff set out to swindle his investors in the beginning.

- 
25. Considering the serious economic downturn in 2008, why do you think the Madoff scheme, and many others also, were discovered around the same time.

- 
26. Research online or elsewhere to find out about other notable Ponzi schemes over the years. Can you identify any common traits among the operators?

EXTENSION Route Planning

Introduction • Minimizing Deadheading

Introduction When planning routes for mail delivery, street sweeping, or snowplowing, the roads in the region to be covered usually do not have an Euler circuit. Unavoidably, certain stretches of road must be traveled more than once. This is referred to as **deadheading**. Planners then try to find a route on which the driver will spend as little time as possible deadheading. We now explore how this can be done.

Minimizing Deadheading In **Example 1**, for simplicity we use street grids for which the distance from corner to corner in any direction is the same.

EXAMPLE 1 Finding an Euler Circuit on a Street Grid

The street grid in **Figure 62** has every vertex of odd degree marked with an X. Insert edges coinciding with existing roads to change it to a graph with an Euler circuit.

SOLUTION

A certain amount of trial and error is needed to find the least number of edges that must be inserted to ensure that the street grid graph has an Euler circuit.

If we insert edges as shown in **Figure 63**, we obtain a graph that has an Euler circuit. (Check that all vertices now have even degree.) This solution introduces 11 edges, which turns out to be more deadheading than is necessary.

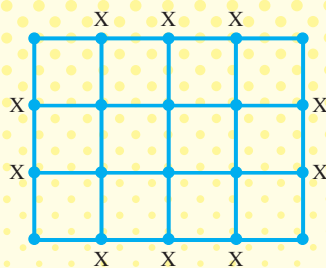
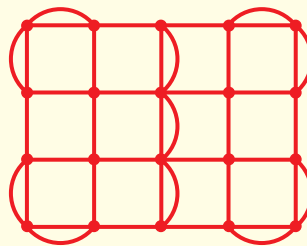
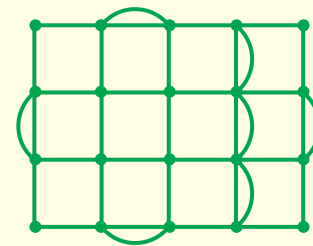


Figure 62



11 edges

Figure 63



7 edges

Figure 64

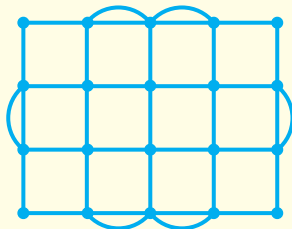
This represents
the least amount
of deadheading.

If we insert edges as shown in **Figure 64**, with just 7 additional edges we obtain a graph with an Euler circuit. This is, in fact, the least number of edges that must be inserted (keeping to the street grid) to change the original street grid graph into a graph that has an Euler circuit. (There are different ways to insert the seven edges.)



EXTENSION EXERCISES

1. In the graph shown here, we have inserted just six edges in the original street grid from **Example 1**. Why is this not a better solution than the one in **Figure 64**?



For each street grid in Exercises 2–4, insert edges to obtain a street grid that has an Euler circuit. Try to insert as few edges as possible.

