CHAPTER

# 4 Number Theory and Cryptography



The part of mathematics devoted to the study of the set of integers and their properties is known as number theory. In this chapter we will develop some of the important concepts of number theory including many of those used in computer science. As we develop number theory, we will use the proof methods developed in Chapter 1 to prove many theorems.

We will first introduce the notion of divisibility of integers, which we use to introduce modular, or clock, arithmetic. Modular arithmetic operates with the remainders of integers when they are divided by a fixed positive integer, called the modulus. We will prove many important results about modular arithmetic which we will use extensively in this chapter.

Integers can be represented with any positive integer $b$ greater than 1 as a base. In this chapter we discuss base $b$ representations of integers and give an algorithm for finding them. In particular, we will discuss binary, octal, and hexadecimal (base 2, 8, and 16) representations. We will describe algorithms for carrying out arithmetic using these representations and study their complexity. These algorithms were the first procedures called algorithms.

We will discuss prime numbers, the positive integers that have only 1 and themselves as positive divisors. We will prove that there are infinitely many primes; the proof we give is considered to be one of the most beautiful proofs in mathematics. We will discuss the distribution of primes and many famous open questions concerning primes. We will introduce the concept of greatest common divisors and study the Euclidean algorithm for computing them. This algorithm was first described thousands of years ago. We will introduce the fundamental theorem of arithmetic, a key result which tells us that every positive integer has a unique factorization into primes.

We will explain how to solve linear congruences, as well as systems of linear congruences, which we solve using the famous Chinese remainder theorem. We will introduce the notion of pseudoprimes, which are composite integers masquerading as primes, and show how this notion can help us rapidly generate prime numbers.

This chapter introduces several important applications of number theory. In particular, we will use number theory to generate pseudorandom numbers, to assign memory locations to computer files, and to find check digits used to detect errors in various kinds of identification numbers. We also introduce the subject of cryptography. Number theory plays an essentially role both in classical cryptography, first used thousands of years ago, and modern cryptography, which plays an essential role in electronic communication. We will show how the ideas we develop can be used in cryptographical protocols, introducing protocols for sharing keys and for sending signed messages. Number theory, once considered the purest of subjects, has become an essential tool in providing computer and Internet security.

## 4.1 Divisibility and Modular Arithmetic

### Introduction

The ideas that we will develop in this section are based on the notion of divisibility. Division of an integer by a positive integer produces a quotient and a remainder. Working with these remainders leads to modular arithmetic, which plays an important role in mathematics and which is used throughout computer science. We will discuss some important applications of modular arithmetic later in this chapter, including generating pseudorandom numbers, assigning computer memory locations to files, constructing check digits, and encrypting messages.

## Division

When one integer is divided by a second nonzero integer, the quotient may or may not be an integer. For example, $12/3 = 4$ is an integer, whereas $11/4 = 2.75$ is not. This leads to Definition 1.

**DEFINITION 1** If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ *divides* $b$ if there is an integer $c$ such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When $a$ divides $b$ we say that $a$ is a *factor* or *divisor* of $b$, and that $b$ is a *multiple* of $a$. The notation $a \mid b$ denotes that $a$ divides $b$. We write $a \nmid b$ when $a$ does not divide $b$.

***Remark:*** We can express $a \mid b$ using quantifiers as $\exists c(ac = b)$, where the universe of discourse is the set of integers.

In Figure 1 a number line indicates which integers are divisible by the positive integer $d$.

**EXAMPLE 1** Determine whether $3 \mid 7$ and whether $3 \mid 12$.

*Solution:* We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$. ◀

**EXAMPLE 2** Let $n$ and $d$ be positive integers. How many positive integers not exceeding $n$ are divisible by $d$?

Extra Examples

*Solution:* The positive integers divisible by $d$ are all the integers of the form $dk$, where $k$ is a positive integer. Hence, the number of positive integers divisible by $d$ that do not exceed $n$ equals the number of integers $k$ with $0 < dk \leq n$, or with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding $n$ that are divisible by $d$. ◀

Some of the basic properties of divisibility of integers are given in Theorem 1.

**THEOREM 1** Let $a$, $b$, and $c$ be integers, where $a \neq 0$. Then

(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(*ii*) if $a \mid b$, then $a \mid bc$ for all integers $c$;
(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

*Proof:* We will give a direct proof of ($i$). Suppose that $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers $s$ and $t$ with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t).$$

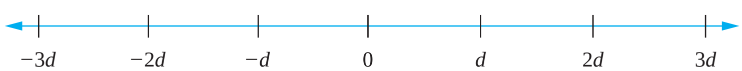


**FIGURE 1** **Integers Divisible by the Positive Integer *d*.**

Therefore, $a$ divides $b + c$. This establishes part ($i$) of the theorem. The proofs of parts ($ii$) and ($iii$) are left as Exercises 3 and 4. ◁

Theorem 1 has this useful consequence.

**COROLLARY 1** If $a$, $b$, and $c$ are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever $m$ and $n$ are integers.

*Proof:* We will give a direct proof. By part ($ii$) of Theorem 1 we see that $a \mid mb$ and $a \mid nc$ whenever $m$ and $n$ are integers. By part ($i$) of Theorem 1 it follows that $a \mid mb + nc$. ◁

## The Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

**THEOREM 2** **THE DIVISION ALGORITHM** Let $a$ be an integer and $d$ a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.

We defer the proof of the division algorithm to Section 5.2. (See Example 5 and Exercise 37.)

***Remark:*** Theorem 2 is not really an algorithm. (Why not?) Nevertheless, we use its traditional name.

**DEFINITION 2** In the equality given in the division algorithm, $d$ is called the *divisor*, $a$ is called the *dividend*, $q$ is called the *quotient*, and $r$ is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

***Remark:*** Note that both $a$ **div** $d$ and $a$ **mod** $d$ for a fixed $d$ are functions on the set of integers. Furthermore, when $a$ is an integer and $d$ is a positive integer, we have $a$ **div** $d = \lfloor a/d \rfloor$ and $a$ **mod** $d = a - d$. (See exercise 18.)

Examples 3 and 4 illustrate the division algorithm.

**EXAMPLE 3** What are the quotient and remainder when 101 is divided by 11?

*Solution:* We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is $9 = 101$ **div** $11$, and the remainder is $2 = 101$ **mod** $11$. ◀

**EXAMPLE 4** What are the quotient and remainder when $-11$ is divided by 3?

*Solution:* We have

$$-11 = 3(-4) + 1.$$

Extra Examples

Hence, the quotient when $-11$ is divided by 3 is $-4 = -11$ **div** 3, and the remainder is $1 = -11$ **mod** 3.

Note that the remainder cannot be negative. Consequently, the remainder is *not* $-2$, even though

$$-11 = 3(-3) - 2,$$

because $r = -2$ does not satisfy $0 \leq r < 3$. ◀

Note that the integer $a$ is divisible by the integer $d$ if and only if the remainder is zero when $a$ is divided by $d$.

***Remark:*** A programming language may have one, or possibly two, operators for modular arithmetic, denoted by mod (in BASIC, Maple, Mathematica, EXCEL, and SQL), % (in C, C++, Java, and Python), rem (in Ada and Lisp), or something else. Be careful when using them, because for $a < 0$, some of these operators return $a - m\lceil a/m \rceil$ instead of $a$ **mod** $m = a - m\lfloor a/m \rfloor$ (as shown in Exercise 18). Also, unlike $a$ **mod** $m$, some of these operators are defined when $m < 0$, and even when $m = 0$.

## Modular Arithmetic

In some situations we care only about the remainder of an integer when it is divided by some specified positive integer. For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have special notations for them. We have already introduced the notation $a$ **mod** $m$ to represent the remainder when an integer $a$ is divided by the positive integer $m$. We now introduce a different, but related, notation that indicates that two integers have the same remainder when they are divided by the positive integer $m$.

**DEFINITION 3** If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is *congruent to $b$ modulo $m$* if $m$ divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that $a$ is congruent to $b$ modulo $m$. We say that $a \equiv b \pmod{m}$ is a **congruence** and that $m$ is its **modulus** (plural **moduli**). If $a$ and $b$ are not congruent modulo $m$, we write $a \not\equiv b \pmod{m}$.

Although both notations $a \equiv b \pmod{m}$ and $a$ **mod** $m = b$ include “mod,” they represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function. However, the relation $a \equiv b \pmod{m}$ and the **mod** $m$ function are closely related, as described in Theorem 3.

**THEOREM 3** Let $a$ and $b$ be integers, and let $m$ be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a$ **mod** $m = b$ **mod** $m$.

The proof of Theorem 3 is left as Exercises 15 and 16. Recall that $a$ **mod** $m$ and $b$ **mod** $m$ are the remainders when $a$ and $b$ are divided by $m$, respectively. Consequently, Theorem 3 also says that $a \equiv b \pmod{m}$ if and only if $a$ and $b$ have the same remainder when divided by $m$.

**EXAMPLE 5** Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

*Solution:* Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$. ◀

The great German mathematician Karl Friedrich Gauss developed the concept of congruences at the end of the eighteenth century. The notion of congruences has played an important role in the development of number theory.

Theorem 4 provides a useful way to work with congruences.

**THEOREM 4** Let $m$ be a positive integer. The integers $a$ and $b$ are congruent modulo $m$ if and only if there is an integer $k$ such that $a = b + km$.

*Proof:* If $a \equiv b \pmod{m}$, by the definition of congruence (Definition 3), we know that $m \mid (a - b)$. This means that there is an integer $k$ such that $a - b = km$, so that $a = b + km$. Conversely, if there is an integer $k$ such that $a = b + km$, then $km = a - b$. Hence, $m$ divides $a - b$, so that $a \equiv b \pmod{m}$. ◁

The set of all integers congruent to an integer $a$ modulo $m$ is called the **congruence class** of $a$ modulo $m$. In Chapter 9 we will show that there are $m$ pairwise disjoint equivalence classes modulo $m$ and that the union of these equivalence classes is the set of integers.

Theorem 5 shows that additions and multiplications preserve congruences.

Links

KARL FRIEDRICH GAUSS (1777–1855) Karl Friedrich Gauss, the son of a bricklayer, was a child prodigy. He demonstrated his potential at the age of 10, when he quickly solved a problem assigned by a teacher to keep the class busy. The teacher asked the students to find the sum of the first 100 positive integers. Gauss realized that this sum could be found by forming 50 pairs, each with the sum 101: $1 + 100, 2 + 99, \ldots, 50 + 51$. This brilliance attracted the sponsorship of patrons, including Duke Ferdinand of Brunswick, who made it possible for Gauss to attend Caroline College and the University of Göttingen. While a student, he invented the method of least squares, which is used to estimate the most likely value of a variable from experimental results. In 1796 Gauss made a fundamental discovery in geometry, advancing a subject that had not advanced since ancient times. He showed that a 17-sided regular polygon could be drawn using just a ruler and compass.

In 1799 Gauss presented the first rigorous proof of the fundamental theorem of algebra, which states that a polynomial of degree $n$ has exactly $n$ roots (counting multiplicities). Gauss achieved worldwide fame when he successfully calculated the orbit of the first asteroid discovered, Ceres, using scanty data.

Gauss was called the Prince of Mathematics by his contemporary mathematicians. Although Gauss is noted for his many discoveries in geometry, algebra, analysis, astronomy, and physics, he had a special interest in number theory, which can be seen from his statement "Mathematics is the queen of the sciences, and the theory of numbers is the queen of mathematics." Gauss laid the foundations for modern number theory with the publication of his book *Disquisitiones Arithmeticae* in 1801.

**THEOREM 5** Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

*Proof:* We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers $s$ and $t$ with $b = a + sm$ and $d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Hence,

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$ ◁

**EXAMPLE 6** Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}.$$ ◂

You cannot always divide both sides of a congruence by the same number!

We must be careful working with congruences. Some properties we may expect to be true are not valid. For example, if $ac \equiv bc \pmod{m}$, the congruence $a \equiv b \pmod{m}$ may be false. Similarly, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the congruence $a^c \equiv b^d \pmod{m}$ may be false. (See Exercise 37.)

Corollary 2 shows how to find the values of the **mod** $m$ function at the sum and product of two integers using the values of this function at each of these integers. We will use this result in Section 5.4.

**COROLLARY 2** Let $m$ be a positive integer and let $a$ and $b$ be integers. Then

$$(a + b) \,\mathbf{mod}\, m = ((a \,\mathbf{mod}\, m) + (b \,\mathbf{mod}\, m)) \,\mathbf{mod}\, m$$

and

$$ab \,\mathbf{mod}\, m = ((a \,\mathbf{mod}\, m)(b \,\mathbf{mod}\, m)) \,\mathbf{mod}\, m.$$

*Proof:* By the definitions of **mod** $m$ and of congruence modulo $m$, we know that $a \equiv (a \,\mathbf{mod}\, m) \pmod{m}$ and $b \equiv (b \,\mathbf{mod}\, m) \pmod{m}$. Hence, Theorem 5 tells us that

$$a + b \equiv (a \,\mathbf{mod}\, m) + (b \,\mathbf{mod}\, m) \pmod{m}$$

and

$$ab \equiv (a \,\mathbf{mod}\, m)(b \,\mathbf{mod}\, m) \pmod{m}.$$

The equalities in this corollary follow from these last two congruences by Theorem 3. ◁

## Arithmetic Modulo *m*

We can define arithmetic operations on $\mathbf{Z}_m$, the set of nonnegative integers less than $m$, that is, the set $\{0, 1, \ldots, m-1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

$$a +_m b = (a + b) \textbf{ mod } m,$$

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by $\cdot_m$ by

$$a \cdot_m b = (a \cdot b) \textbf{ mod } m,$$

where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers. The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo $m$ and when we use these operations, we are said to be doing **arithmetic modulo** $m$.

**EXAMPLE 7** Use the definition of addition and multiplication in $\mathbf{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

*Solution:* Using the definition of addition modulo 11, we find that

$$7 +_{11} 9 = (7 + 9) \textbf{ mod } 11 = 16 \textbf{ mod } 11 = 5,$$

and

$$7 \cdot_{11} 9 = (7 \cdot 9) \textbf{ mod } 11 = 63 \textbf{ mod } 11 = 8.$$

Hence $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$. ◀

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers. In particular, they satisfy these properties:

**Closure** If $a$ and $b$ belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.

**Associativity** If $a$, $b$, and $c$ belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

**Commutativity** If $a$ and $b$ belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

**Identity elements** The elements 0 and 1 are identity elements for addition and multiplication modulo $m$, respectively. That is, if $a$ belongs to $\mathbf{Z}_m$, then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.

**Additive inverses** If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is an additive inverse of $a$ modulo $m$ and 0 is its own additive inverse. That is $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

**Distributivity** If $a$, $b$, and $c$ belong to $\mathbf{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

These properties follow from the properties we have developed for congruences and remainders modulo $m$, together with the properties of integers; we leave their proofs as Exercises 42–44. Note that we have listed the property that every element of $\mathbf{Z}_m$ has an additive inverse, but no analogous property for multiplicative inverses has been included. This is because multiplicative inverses do not always exists modulo $m$. For instance, there is no multiplicative inverse of 2 modulo 6, as the reader can verify. We will return to the question of when an integer has a multiplicative inverse modulo $m$ later in this chapter.

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

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

## Exercises

**1.** Does 17 divide each of these numbers?
**a)** 68 **b)** 84 **c)** 357 **d)** 1001

**2.** Prove that if $a$ is an integer other than 0, then
**a)** 1 divides $a$. **b)** $a$ divides 0.

**3.** Prove that part (*ii*) of Theorem 1 is true.

**4.** Prove that part (*iii*) of Theorem 1 is true.

**5.** Show that if $a \mid b$ and $b \mid a$, where $a$ and $b$ are integers, then $a = b$ or $a = -b$.

**6.** Show that if $a$, $b$, $c$, and $d$ are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

**7.** Show that if $a$, $b$, and $c$ are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.

**8.** Prove or disprove that if $a \mid bc$, where $a$, $b$, and $c$ are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.

**9.** What are the quotient and remainder when
**a)** 19 is divided by 7?
**b)** $-111$ is divided by 11?
**c)** 789 is divided by 23?
**d)** 1001 is divided by 13?
**e)** 0 is divided by 19?
**f)** 3 is divided by 5?
**g)** $-1$ is divided by 3?
**h)** 4 is divided by 1?

**10.** What are the quotient and remainder when
**a)** 44 is divided by 8?
**b)** 777 is divided by 21?
**c)** $-123$ is divided by 19?
**d)** $-1$ is divided by 23?
**e)** $-2002$ is divided by 87?
**f)** 0 is divided by 17?
**g)** 1,234,567 is divided by 1001?
**h)** $-100$ is divided by 101?

**11.** What time does a 12-hour clock read
**a)** 80 hours after it reads 11:00?
**b)** 40 hours before it reads 12:00?
**c)** 100 hours after it reads 6:00?

**12.** What time does a 24-hour clock read
**a)** 100 hours after it reads 2:00?
**b)** 45 hours before it reads 12:00?
**c)** 168 hours after it reads 19:00?

**13.** Suppose that $a$ and $b$ are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer $c$ with $0 \leq c \leq 12$ such that
**a)** $c \equiv 9a \pmod{13}$.
**b)** $c \equiv 11b \pmod{13}$.
**c)** $c \equiv a + b \pmod{13}$.
**d)** $c \equiv 2a + 3b \pmod{13}$.
**e)** $c \equiv a^2 + b^2 \pmod{13}$.
**f)** $c \equiv a^3 - b^3 \pmod{13}$.

**14.** Suppose that $a$ and $b$ are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer $c$ with $0 \leq c \leq 18$ such that
**a)** $c \equiv 13a \pmod{19}$.
**b)** $c \equiv 8b \pmod{19}$.
**c)** $c \equiv a - b \pmod{19}$.
**d)** $c \equiv 7a + 3b \pmod{19}$.
**e)** $c \equiv 2a^2 + 3b^2 \pmod{19}$.
**f)** $c \equiv a^3 + 4b^3 \pmod{19}$.

**15.** Let $m$ be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \mathbin{\mathbf{mod}} m = b \mathbin{\mathbf{mod}} m$.

**16.** Let $m$ be a positive integer. Show that $a \mathbin{\mathbf{mod}} m = b \mathbin{\mathbf{mod}} m$ if $a \equiv b \pmod{m}$.

**17.** Show that if $n$ and $k$ are positive integers, then $\lceil n/k \rceil = \lfloor (n-1)/k \rfloor + 1$.

**18.** Show that if $a$ is an integer and $d$ is an integer greater than 1, then the quotient and remainder obtained when $a$ is divided by $d$ are $\lfloor a/d \rfloor$ and $a - d\lfloor a/d \rfloor$, respectively.

**19.** Find a formula for the integer with smallest absolute value that is congruent to an integer $a$ modulo $m$, where $m$ is a positive integer.

**20.** Evaluate these quantities.
**a)** $-17 \mathbin{\mathbf{mod}} 2$ **b)** $144 \mathbin{\mathbf{mod}} 7$
**c)** $-101 \mathbin{\mathbf{mod}} 13$ **d)** $199 \mathbin{\mathbf{mod}} 19$

**21.** Evaluate these quantities.
**a)** $13 \mathbin{\mathbf{mod}} 3$ **b)** $-97 \mathbin{\mathbf{mod}} 11$
**c)** $155 \mathbin{\mathbf{mod}} 19$ **d)** $-221 \mathbin{\mathbf{mod}} 23$

**22.** Find $a \mathbin{\mathbf{div}} m$ and $a \mathbin{\mathbf{mod}} m$ when
**a)** $a = -111$, $m = 99$.
**b)** $a = -9999$, $m = 101$.
**c)** $a = 10299$, $m = 999$.
**d)** $a = 123456$, $m = 1001$.

**23.** Find $a$ **div** $m$ and $a$ **mod** $m$ when
  **a)** $a = 228$, $m = 119$.
  **b)** $a = 9009$, $m = 223$.
  **c)** $a = -10101$, $m = 333$.
  **d)** $a = -765432$, $m = 38271$.

**24.** Find the integer $a$ such that
  **a)** $a \equiv 43 \pmod{23}$ and $-22 \le a \le 0$.
  **b)** $a \equiv 17 \pmod{29}$ and $-14 \le a \le 14$.
  **c)** $a \equiv -11 \pmod{21}$ and $90 \le a \le 110$.

**25.** Find the integer $a$ such that
  **a)** $a \equiv -15 \pmod{27}$ and $-26 \le a \le 0$.
  **b)** $a \equiv 24 \pmod{31}$ and $-15 \le a \le 15$.
  **c)** $a \equiv 99 \pmod{41}$ and $100 \le a \le 140$.

**26.** List five integers that are congruent to 4 modulo 12.

**27.** List all integers between $-100$ and 100 that are congruent to $-1$ modulo 25.

**28.** Decide whether each of these integers is congruent to 3 modulo 7.
  **a)** 37 **b)** 66
  **c)** $-17$ **d)** $-67$

**29.** Decide whether each of these integers is congruent to 5 modulo 17.
  **a)** 80 **b)** 103
  **c)** $-29$ **d)** $-122$

**30.** Find each of these values.
  **a)** $(177 \textbf{ mod } 31 + 270 \textbf{ mod } 31) \textbf{ mod } 31$
  **b)** $(177 \textbf{ mod } 31 \cdot 270 \textbf{ mod } 31) \textbf{ mod } 31$

**31.** Find each of these values.
  **a)** $(-133 \textbf{ mod } 23 + 261 \textbf{ mod } 23) \textbf{ mod } 23$
  **b)** $(457 \textbf{ mod } 23 \cdot 182 \textbf{ mod } 23) \textbf{ mod } 23$

**32.** Find each of these values.
  **a)** $(19^2 \textbf{ mod } 41) \textbf{ mod } 9$
  **b)** $(32^3 \textbf{ mod } 13)^2 \textbf{ mod } 11$
  **c)** $(7^3 \textbf{ mod } 23)^2 \textbf{ mod } 31$
  **d)** $(21^2 \textbf{ mod } 15)^3 \textbf{ mod } 22$

**33.** Find each of these values.
  **a)** $(99^2 \textbf{ mod } 32)^3 \textbf{ mod } 15$
  **b)** $(3^4 \textbf{ mod } 17)^2 \textbf{ mod } 11$
  **c)** $(19^3 \textbf{ mod } 23)^2 \textbf{ mod } 31$
  **d)** $(89^3 \textbf{ mod } 79)^4 \textbf{ mod } 26$

**34.** Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where $a$, $b$, $c$, $d$, and $m$ are integers with $m \ge 2$, then $a - c \equiv b - d \pmod{m}$.

**35.** Show that if $n \mid m$, where $n$ and $m$ are integers greater than 1, and if $a \equiv b \pmod{m}$, where $a$ and $b$ are integers, then $a \equiv b \pmod{n}$.

**36.** Show that if $a$, $b$, $c$, and $m$ are integers such that $m \ge 2$, $c > 0$, and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.

**37.** Find counterexamples to each of these statements about congruences.
  **a)** If $ac \equiv bc \pmod{m}$, where $a$, $b$, $c$, and $m$ are integers with $m \ge 2$, then $a \equiv b \pmod{m}$.
  **b)** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where $a$, $b$, $c$, $d$, and $m$ are integers with $c$ and $d$ positive and $m \ge 2$, then $a^c \equiv b^d \pmod{m}$.

**38.** Show that if $n$ is an integer then $n^2 \equiv 0$ or $1 \pmod{4}$.

**39.** Use Exercise 38 to show that if $m$ is a positive integer of the form $4k + 3$ for some nonnegative integer $k$, then $m$ is not the sum of the squares of two integers.

**40.** Prove that if $n$ is an odd positive integer, then $n^2 \equiv 1 \pmod{8}$.

**41.** Show that if $a$, $b$, $k$, and $m$ are integers such that $k \ge 1$, $m \ge 2$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

**42.** Show that $\mathbf{Z}_m$ with addition modulo $m$, where $m \ge 2$ is an integer, satisfies the closure, associative, and commutative properties, 0 is an additive identity, and for every nonzero $a \in \mathbf{Z}_m$, $m - a$ is an inverse of $a$ modulo $m$.

**43.** Show that $\mathbf{Z}_m$ with multiplication modulo $m$, where $m \ge 2$ is an integer, satisfies the closure, associative, and commutativity properties, and 1 is a multiplicative identity.

**44.** Show that the distributive property of multiplication over addition holds for $\mathbf{Z}_m$, where $m \ge 2$ is an integer.

**45.** Write out the addition and multiplication tables for $\mathbf{Z}_5$ (where by addition and multiplication we mean $+_5$ and $\cdot_5$).

**46.** Write out the addition and multiplication tables for $\mathbf{Z}_6$ (where by addition and multiplication we mean $+_6$ and $\cdot_6$).

**47.** Determine whether each of the functions $f(a) = a \textbf{ div } d$ and $g(a) = a \textbf{ mod } d$, where $d$ is a fixed positive integer, from the set of integers to the set of integers, is one-to-one, and determine whether each of these functions is onto.

# 4.2 Integer Representations and Algorithms

## Introduction

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

**55.** Devise an algorithm that, given the binary expansions of the integers $a$ and $b$, determines whether $a > b$, $a = b$, or $a < b$.

**56.** How many bit operations does the comparison algorithm from Exercise 55 use when the larger of $a$ and $b$ has $n$ bits in its binary expansion?

**57.** Estimate the complexity of Algorithm 1 for finding the base $b$ expansion of an integer $n$ in terms of the number of divisions used.

***58.** Show that Algorithm 5 uses $O((\log m)^2 \log n)$ bit operations to find $b^n$ **mod** $m$.

**59.** Show that Algorithm 4 uses $O(q \log a)$ bit operations, assuming that $a > d$.

# 4.3 Primes and Greatest Common Divisors

## Introduction

In Section 4.1 we studied the concept of divisibility of integers. One important concept based on divisibility is that of a prime number. A prime is an integer greater than 1 that is divisible by no positive integers other than 1 and itself. The study of prime numbers goes back to ancient times. Thousands of years ago it was known that there are infinitely many primes; the proof of this fact, found in the works of Euclid, is famous for its elegance and beauty.

We will discuss the distribution of primes among the integers. We will describe some of the results about primes found by mathematicians in the last 400 years. In particular, we will introduce an important theorem, the fundamental theorem of arithmetic. This theorem, which asserts that every positive integer can be written uniquely as the product of primes in nondecreasing order, has many interesting consequences. We will also discuss some of the many old conjectures about primes that remain unsettled today.

Primes have become essential in modern cryptographic systems, and we will develop some of their properties important in cryptography. For example, finding large primes is essential in modern cryptography. The length of time required to factor large integers into their prime factors is the basis for the strength of some important modern cryptographic systems.

In this section we will also study the greatest common divisor of two integers, as well as the least common multiple of two integers. We will develop an important algorithm for computing greatest common divisors, called the Euclidean algorithm.

## Primes

Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called **primes**.

**DEFINITION 1** An integer $p$ greater than 1 is called *prime* if the only positive factors of $p$ are 1 and $p$. A positive integer that is greater than 1 and is not prime is called *composite*.

***Remark:*** The integer $n$ is composite if and only if there exists an integer $a$ such that $a \mid n$ and $1 < a < n$.

**EXAMPLE 1** The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3. ◀

The primes are the building blocks of positive integers, as the fundamental theorem of arithmetic shows. The proof will be given in Section 5.2.

**THEOREM 1** **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example 2 gives some prime factorizations of integers.

**EXAMPLE 2** The prime factorizations of 100, 641, 999, and 1024 are given by

Extra Examples

$$\begin{aligned}
100 &= 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2, \\
641 &= 641, \\
999 &= 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37, \\
1024 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.
\end{aligned}$$

◀

## Trial Division

It is often important to show that a given integer is prime. For instance, in cryptology, large primes are used in some methods for making messages secret. One procedure for showing that an integer is prime is based on the following observation.

**THEOREM 2** If $n$ is a composite integer, then $n$ has a prime divisor less than or equal to $\sqrt{n}$.

*Proof:* If $n$ is composite, by the definition of a composite integer, we know that it has a factor $a$ with $1 < a < n$. Hence, by the definition of a factor of a positive integer, we have $n = ab$, where $b$ is a positive integer greater than 1. We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Because both $a$ and $b$ are divisors of $n$, we see that $n$ has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, $n$ has a prime divisor less than or equal to $\sqrt{n}$. ◁

From Theorem 2, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. This leads to the brute-force algorithm known as **trial division**. To use trial division we divide $n$ by all primes not exceeding $\sqrt{n}$ and conclude that $n$ is prime if it is not divisible by any of these primes. In Example 3 we use trial division to show that 101 is prime.

**EXAMPLE 3** Show that 101 is prime.

*Solution:* The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime. ◀

Because every integer has a prime factorization, it would be useful to have a procedure for finding this prime factorization. Consider the problem of finding the prime factorization of $n$. Begin by dividing $n$ by successive primes, starting with the smallest prime, 2. If $n$ has a prime factor, then by Theorem 3 a prime factor $p$ not exceeding $\sqrt{n}$ will be found. So, if no prime factor not exceeding $\sqrt{n}$ is found, then $n$ is prime. Otherwise, if a prime factor $p$ is found, continue by factoring $n/p$. Note that $n/p$ has no prime factors less than $p$. Again, if $n/p$ has no prime factor greater than or equal to $p$ and not exceeding its square root, then it is prime. Otherwise, if it has a prime factor $q$, continue by factoring $n/(pq)$. This procedure is continued until the factorization has been reduced to a prime. This procedure is illustrated in Example 4.

**EXAMPLE 4** Find the prime factorization of 7007.

*Solution:* To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$. Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$. ◀

Prime numbers were studied in ancient times for philosophical reasons. Today, there are highly practical reasons for their study. In particular, large primes play a crucial role in cryptography, as we will see in Section 4.6.

## The Sieve of Eratosthenes

Note that composite integers not exceeding 100 must have a prime factor not exceeding 10. Because the only primes less than 10 are 2, 3, 5, and 7, the primes not exceeding 100 are these four primes and those positive integers greater than 1 and not exceeding 100 that are divisible by none of 2, 3, 5, or 7.

The **sieve of Eratosthenes** is used to find all primes not exceeding a specified positive integer. For instance, the following procedure is used to find the primes not exceeding 100. We begin with the list of all integers between 1 and 100. To begin the sieving process, the integers that are divisible by 2, other than 2, are deleted. Because 3 is the first integer greater than 2 that is left, all those integers divisible by 3, other than 3, are deleted. Because 5 is the next integer left after 3, those integers divisible by 5, other than 5, are deleted. The next integer left is 7, so those integers divisible by 7, other than 7, are deleted. Because all composite integers not exceeding 100 are divisible by 2, 3, 5, or 7, all remaining integers except 1 are prime. In Table 1, the panels display those integers deleted at each stage, where each integer divisible by 2, other than 2, is underlined in the first panel, each integer divisible by 3, other than 3, is underlined in the second panel, each integer divisible by 5, other than 5, is underlined in the third panel, and each integer divisible by 7, other than 7, is underlined in the fourth panel. The integers not underlined are the primes not exceeding 100. We conclude that the primes less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

THE INFINITUDE OF PRIMES It has long been known that there are infinitely many primes. This means that whenever $p_1, p_2, \ldots, p_n$ are the $n$ smallest primes, we know there is a larger

ERATOSTHENES (276 B.C.E.–194 B.C.E.) It is known that Eratosthenes was born in Cyrene, a Greek colony west of Egypt, and spent time studying at Plato's Academy in Athens. We also know that King Ptolemy II invited Eratosthenes to Alexandria to tutor his son and that later Eratosthenes became chief librarian at the famous library at Alexandria, a central repository of ancient wisdom. Eratosthenes was an extremely versatile scholar, writing on mathematics, geography, astronomy, history, philosophy, and literary criticism. Besides his work in mathematics, he is most noted for his chronology of ancient history and for his famous measurement of the size of the earth.

**TABLE 1** **The Sieve of Eratosthenes.**

***Integers divisible by 2 other than 2 receive an underline.***

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

***Integers divisible by 3 other than 3 receive an underline.***

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

***Integers divisible by 5 other than 5 receive an underline.***

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

***Integers divisible by 7 other than 7 receive an underline; integers in color are prime.***

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

prime not listed. We will prove this fact using a proof given by Euclid in his famous mathematics text, *The Elements*. This simple, yet elegant, proof is considered by many mathematicians to be among the most beautiful proofs in mathematics. It is the first proof presented in the book *Proofs from THE BOOK* [AiZi10], where THE BOOK refers to the imagined collection of perfect proofs that the famous mathematician Paul Erdős claimed is maintained by God. By the way, there are a vast number of different proofs than there are an infinitude of primes, and new ones are published surprisingly frequently.

**THEOREM 3** There are infinitely many primes.

***Proof:*** We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 p_2 \cdots p_n + 1.$$

By the fundamental theorem of arithmetic, $Q$ is prime or else it can be written as the product of two or more primes. However, none of the primes $p_j$ divides $Q$, for if $p_j \mid Q$, then $p_j$ divides

$Q - p_1 p_2 \cdots p_n = 1$. Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either $Q$, if it is prime, or a prime factor of $Q$. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes. ◁

***Remark:*** Note that in this proof we do *not* state that $Q$ is prime! Furthermore, in this proof, we have given a nonconstructive existence proof that given any $n$ primes, there is a prime not in this list. For this proof to be constructive, we would have had to explicitly give a prime not in our original list of $n$ primes.

Because there are infinitely many primes, given any positive integer there are primes greater than this integer. There is an ongoing quest to discover larger and larger prime numbers; for almost all the last 300 years, the largest prime known has been an integer of the special form $2^p - 1$, where $p$ is also prime. (Note that $2^n - 1$ cannot be prime when $n$ is not prime; see Exercise 9.) Such primes are called **Mersenne primes**, after the French monk Marin Mersenne, who studied them in the seventeenth century. The reason that the largest known prime has usually been a Mersenne prime is that there is an extremely efficient test, known as the Lucas–Lehmer test, for determining whether $2^p - 1$ is prime. Furthermore, it is not currently possible to test numbers not of this or certain other special forms anywhere near as quickly to determine whether they are prime.

**EXAMPLE 5** The numbers $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are Mersenne primes, while $2^{11} - 1 = 2047$ is not a Mersenne prime because $2047 = 23 \cdot 89$. ◀

Links

Progress in finding Mersenne primes has been steady since computers were invented. As of early 2011, 47 Mersenne primes were known, with 16 found since 1990. The largest Mersenne prime known (again as of early 2011) is $2^{43,112,609} - 1$, a number with nearly 13 million decimal digits, which was shown to be prime in 2008. A communal effort, the Great Internet Mersenne Prime Search (GIMPS), is devoted to the search for new Mersenne primes. You can join this search, and if you are lucky, find a new Mersenne prime and possibly even win a cash prize. By the way, even the search for Mersenne primes has practical implications. One quality control test for supercomputers has been to replicate the Lucas–Lehmer test that establishes the primality of a large Mersenne prime. (See [Ro10] for more information about the quest for finding Mersenne primes.)

THE DISTRIBUTION OF PRIMES Theorem 3 tells us that there are infinitely many primes. However, how many primes are less than a positive number $x$? This question interested mathematicians for many years; in the late eighteenth century, mathematicians produced large tables

Links

MARIN MERSENNE (1588–1648) Mersenne was born in Maine, France, into a family of laborers and attended the College of Mans and the Jesuit College at La Flèche. He continued his education at the Sorbonne, studying theology from 1609 to 1611. He joined the religious order of the Minims in 1611, a group whose name comes from the word *minimi* (the members of this group were extremely humble; they considered themselves the least of all religious orders). Besides prayer, the members of this group devoted their energy to scholarship and study. In 1612 he became a priest at the Place Royale in Paris; between 1614 and 1618 he taught philosophy at the Minim Convent at Nevers. He returned to Paris in 1619, where his cell in the Minims de l'Annociade became a place for meetings of French scientists, philosophers, and mathematicians, including Fermat and Pascal. Mersenne corresponded extensively with scholars throughout Europe, serving as a clearinghouse for mathematical and scientific knowledge, a function later served by mathematical journals (and today also by the Internet). Mersenne wrote books covering mechanics, mathematical physics, mathematics, music, and acoustics. He studied prime numbers and tried unsuccessfully to construct a formula representing all primes. In 1644 Mersenne claimed that $2^p - 1$ is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ but is composite for all other primes less than 257. It took over 300 years to determine that Mersenne's claim was wrong five times. Specifically, $2^p - 1$ is not prime for $p = 67$ and $p = 257$ but is prime for $p = 61$, $p = 87$, and $p = 107$. It is also noteworthy that Mersenne defended two of the most famous men of his time, Descartes and Galileo, from religious critics. He also helped expose alchemists and astrologers as frauds.

of prime numbers to gather evidence concerning the distribution of primes. Using this evidence, the great mathematicians of the day, including Gauss and Legendre, conjectured, but did not prove, Theorem 4.

**THEOREM 4** **THE PRIME NUMBER THEOREM** The ratio of the number of primes not exceeding $x$ and $x/\ln x$ approaches 1 as $x$ grows without bound. (Here $\ln x$ is the natural logarithm of $x$.)

Links

The prime number theorem was first proved in 1896 by the French mathematician Jacques Hadamard and the Belgian mathematician Charles-Jean-Gustave-Nicholas de la Vallée-Poussin using the theory of complex variables. Although proofs not using complex variables have been found, all known proofs of the prime number theorem are quite complicated.

We can use the prime number theorem to estimate the odds that a randomly chosen number is prime. The prime number theorem tells us that the number of primes not exceeding $x$ can be approximated by $x/\ln x$. Consequently, the odds that a randomly selected positive integer less than $n$ is prime are approximately $(n/\ln n)/n = 1/\ln n$. Sometimes we need to find a prime with a particular number of digits. We would like an estimate of how many integers with a particular number of digits we need to select before we encounter a prime. Using the prime number theorem and calculus, it can be shown that the probability that an integer $n$ is prime is also approximately $1/\ln n$. For example, the odds that an integer near $10^{1000}$ is prime are approximately $1/\ln 10^{1000}$, which is approximately 1/2300. (Of course, by choosing only odd numbers, we double our chances of finding a prime.)

Using trial division with Theorem 2 gives procedures for factoring and for primality testing. However, these procedures are not efficient algorithms; many much more practical and efficient algorithms for these tasks have been developed. Factoring and primality testing have become important in the applications of number theory to cryptography. This has led to a great interest in developing efficient algorithms for both tasks. Clever procedures have been devised in the last 30 years for efficiently generating large primes. Moreover, in 2002, an important theoretical discovery was made by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. They showed there is a polynomial-time algorithm in the number of bits in the binary expansion of an integer for determining whether a positive integer is prime. Algorithms based on their work use $O((\log n)^6)$ bit operations to determine whether a positive integer $n$ is prime.

However, even though powerful new factorization methods have been developed in the same time frame, factoring large numbers remains extraordinarily more time-consuming than primality testing. No polynomial-time algorithm for factoring integers is known. Nevertheless, the challenge of factoring large numbers interests many people. There is a communal effort on the Internet to factor large numbers, especially those of the special form $k^n \pm 1$, where $k$ is a small positive integer and $n$ is a large positive integer (such numbers are called *Cunningham numbers*). At any given time, there is a list of the "Ten Most Wanted" large numbers of this type awaiting factorization.

**PRIMES AND ARITHMETIC PROGRESSIONS** Every odd integer is in one of the two arithmetic progressions $4k + 1$ or $4k + 3$, $k = 1, 2, \ldots$. Because we know that there are infinitely many primes, we can ask whether there are infinitely many primes in both of these arithmetic progressions. The primes $5, 13, 17, 29, 37, 41, \ldots$ are in the arithmetic progression $4k + 1$; the primes $3, 7, 11, 19, 23, 31, 43, \ldots$ are in the arithmetic progression $4k + 3$. Looking at the evidence hints that there may be infinitely many primes in both progressions. What about other arithmetic progressions $ak + b$, $k = 1, 2, \ldots$, where no integer greater than one divides both $a$ and $b$? Do they contain infinitely many primes? The answer was provided by the German mathematician G. Lejeune Dirichlet, who proved that every such arithmetic progression contains infinitely many primes. His proof, and all proofs found later, are beyond the scope of this book.

However, it is possible to prove special cases of Dirichlet's theorem using the ideas developed in this book. For example, Exercises 54 and 55 ask for proofs that there are infinitely many primes in the arithmetic progressions $3k + 2$ and $4k + 3$, where $k$ is a positive integer. (The hint for each of these exercises supplies the basic idea needed for the proof.)

We have explained that every arithmetic progression $ak + b$, $k = 1, 2, \ldots$, where $a$ and $b$ have no common factor greater than one, contains infinitely many primes. But are there long arithmetic progressions made up of just primes? For example, some exploration shows that 5, 11, 17, 23, 29 is an arithmetic progression of five primes and 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 is an arithmetic progression of ten primes. In the 1930s, the famous mathematician Paul Erdős conjectured that for every positive integer $n$ greater than two, there is an arithmetic progression of length $n$ made up entirely of primes. In 2006, Ben Green and Terence Tao were able to prove this conjecture. Their proof, considered to be a mathematical tour de force, is a nonconstructive proof that combines powerful ideas from several advanced areas of mathematics.

## Conjectures and Open Problems About Primes

Number theory is noted as a subject for which it is easy to formulate conjectures, some of which are difficult to prove and others that remained open problems for many years. We will describe some conjectures in number theory and discuss their status in Examples 6–9.

**EXAMPLE 6** Extra Examples

It would be useful to have a function $f(n)$ such that $f(n)$ is prime for all positive integers $n$. If we had such a function, we could find large primes for use in cryptography and other applications. Looking for such a function, we might check out different polynomial functions, as some mathematicians did several hundred years ago. After a lot of computation we may encounter the polynomial $f(n) = n^2 - n + 41$. This polynomial has the interesting property that $f(n)$ is prime for all positive integers $n$ not exceeding 40. [We have $f(1) = 41$, $f(2) = 43$, $f(3) = 47$, $f(4) = 53$, and so on.] This can lead us to the conjecture that $f(n)$ is prime for all positive integers $n$. Can we settle this conjecture?

*Solution:* Perhaps not surprisingly, this conjecture turns out to be false; we do not have to look far to find a positive integer $n$ for which $f(n)$ is composite, because $f(41) = 41^2 - 41 + 41 = 41^2$. Because $f(n) = n^2 - n + 41$ is prime for all positive integers $n$ with $1 \leq n \leq 40$, we might

TERENCE TAO (BORN 1975) Tao was born in Australia. His father is a pediatrician and his mother taught mathematics at a Hong Kong secondary school. Tao was a child prodigy, teaching himself arithmetic at the age of two. At 10, he became the youngest contestant at the International Mathematical Olympiad (IMO); he won an IMO gold medal at 13. Tao received his bachelors and masters degrees when he was 17, and began graduate studies at Princeton, receiving his Ph.D. in three years. In 1996 he became a faculty member at UCLA, where he continues to work.

Tao is extremely versatile; he enjoys working on problems in diverse areas, including harmonic analysis, partial differential equations, number theory, and combinatorics. You can follow his work by reading his blog where he discusses progress on various problems. His most famous result is the Green-Tao theorem, which says that there are arbitrarily long arithmetic progressions of primes. Tao has made important contributions to the applications of mathematics, such as developing a method for reconstructing digital images using the least possible amount of information.

Tao has an amazing reputation among mathematicians; he has become a Mr. Fix-It for researchers in mathematics. The well-known mathematician Charles Fefferman, himself a child prodigy, has said that "if you're stuck on a problem, then one way out is to interest Terence Tao." In 2006 Tao was awarded a Fields Medal, the most prestigious award for mathematicians under the age of 40. He was also awarded a MacArthur Fellowship in 2006, and in 2008, he received the Allan T. Waterman award, which came with a $500,000 cash prize to support research work of scientists early in their career. Tao's wife Laura is an engineer at the Jet Propulsion Laboratory.

be tempted to find a different polynomial with the property that $f(n)$ is prime for *all* positive integers $n$. However, there is no such polynomial. It can be shown that for every polynomial $f(n)$ with integer coefficients, there is a positive integer $y$ such that $f(y)$ is composite. (See Exercise 23 in the Supplementary Exercises.)

Many famous problems about primes still await ultimate resolution by clever people. We describe a few of the most accessible and better known of these open problems in Examples 7–9. Number theory is noted for its wealth of easy-to-understand conjectures that resist attack by all but the most sophisticated techniques, or simply resist all attacks. We present these conjectures to show that many questions that seem relatively simple remain unsettled even in the twenty-first century.

**EXAMPLE 7** **Goldbach's Conjecture** In 1742, Christian Goldbach, in a letter to Leonhard Euler, conjectured that every odd integer $n$, $n > 5$, is the sum of three primes. Euler replied that this conjecture is equivalent to the conjecture that every even integer $n$, $n > 2$, is the sum of two primes (see Exercise 21 in the Supplementary Exercises). The conjecture that every even integer $n$, $n > 2$, is the sum of two primes is now called **Goldbach's conjecture**. We can check this conjecture for small even numbers. For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 7 + 5$, and so on. Goldbach's conjecture was verified by hand calculations for numbers up to the millions prior to the advent of computers. With computers it can be checked for extremely large numbers. As of mid 2011, the conjecture has been checked for all positive even integers up to $1.6 \cdot 10^{18}$.

Although no proof of Goldbach's conjecture has been found, most mathematicians believe it is true. Several theorems have been proved, using complicated methods from analytic number theory far beyond the scope of this book, establishing results weaker than Goldbach's conjecture. Among these are the result that every even integer greater than 2 is the sum of at most six primes (proved in 1995 by O. Ramaré) and that every sufficiently large positive integer is the sum of a prime and a number that is either prime or the product of two primes (proved in 1966 by J. R. Chen). Perhaps Goldbach's conjecture will be settled in the not too distant future.

**EXAMPLE 8** There are many conjectures asserting that there are infinitely many primes of certain special forms. A conjecture of this sort is the conjecture that there are infinitely many primes of the form $n^2 + 1$, where $n$ is a positive integer. For example, $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$, and so on. The best result currently known is that there are infinitely many positive integers $n$ such that $n^2 + 1$ is prime or the product of at most two primes (proved by Henryk Iwaniec in 1973 using advanced techniques from analytic number theory, far beyond the scope of this book).

**EXAMPLE 9** **The Twin Prime Conjecture** **Twin primes** are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, and 4967 and 4969. The twin prime conjecture asserts that there are infinitely many twin primes. The strongest result proved concerning twin primes is that there are infinitely many pairs $p$ and $p + 2$, where $p$ is prime and $p + 2$ is prime or the product of two primes (proved by J. R. Chen in 1966). The world's record for twin primes, as of mid 2011, consists of the numbers $65{,}516{,}468{,}355 \cdot 2^{333{,}333} \pm 1$, which have 100,355 decimal digits.

CHRISTIAN GOLDBACH (1690–1764) Christian Goldbach was born in Königsberg, Prussia, the city noted for its famous bridge problem (which will be studied in Section 10.5). He became professor of mathematics at the Academy in St. Petersburg in 1725. In 1728 Goldbach went to Moscow to tutor the son of the Tsar. He entered the world of politics when, in 1742, he became a staff member in the Russian Ministry of Foreign Affairs. Goldbach is best known for his correspondence with eminent mathematicians, including Euler and Bernoulli, for his famous conjectures in number theory, and for several contributions to analysis.

## Greatest Common Divisors and Least Common Multiples

The largest integer that divides both of two integers is called the **greatest common divisor** of these integers.

**DEFINITION 2** Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of $a$ and $b$. The greatest common divisor of $a$ and $b$ is denoted by $\gcd(a, b)$.

The greatest common divisor of two integers, not both zero, exists because the set of common divisors of these integers is nonempty and finite. One way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor. This is done in Examples 10 and 11. Later, a more efficient method of finding greatest common divisors will be given.

**EXAMPLE 10** What is the greatest common divisor of 24 and 36?

*Solution:* The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, $\gcd(24, 36) = 12$. ◀

**EXAMPLE 11** What is the greatest common divisor of 17 and 22?

*Solution:* The integers 17 and 22 have no positive common divisors other than 1, so that $\gcd(17, 22) = 1$. ◀

Because it is often important to specify that two integers have no common positive divisor other than 1, we have Definition 3.

**DEFINITION 3** The integers $a$ and $b$ are *relatively prime* if their greatest common divisor is 1.

**EXAMPLE 12** By Example 11 it follows that the integers 17 and 22 are relatively prime, because $\gcd(17, 22) = 1$. ◀

Because we often need to specify that no two integers in a set of integers have a common positive divisor greater than 1, we make Definition 4.

**DEFINITION 4** The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

**EXAMPLE 13** Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

*Solution:* Because $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, and $\gcd(17, 21) = 1$, we conclude that 10, 17, and 21 are pairwise relatively prime.

Because $\gcd(10, 24) = 2 > 1$, we see that 10, 19, and 24 are not pairwise relatively prime. ◀

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers $a$ and $b$ are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},\ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either $a$ or $b$ are included in both factorizations, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

where $\min(x, y)$ represents the minimum of the two numbers $x$ and $y$. To show that this formula for $\gcd(a, b)$ is valid, we must show that the integer on the right-hand side divides both $a$ and $b$, and that no larger integer also does. This integer does divide both $a$ and $b$, because the power of each prime in the factorization does not exceed the power of this prime in either the factorization of $a$ or that of $b$. Further, no larger integer can divide both $a$ and $b$, because the exponents of the primes in this factorization cannot be increased, and no other primes can be included.

**EXAMPLE 14** Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is

$$\gcd(120, 500) = 2^{\min(3,\,2)} 3^{\min(1,\,0)} 5^{\min(1,\,3)} = 2^2 3^0 5^1 = 20.$$ ◀

Prime factorizations can also be used to find the **least common multiple** of two integers.

**DEFINITION 5** The *least common multiple* of the positive integers $a$ and $b$ is the smallest positive integer that is divisible by both $a$ and $b$. The least common multiple of $a$ and $b$ is denoted by $\operatorname{lcm}(a, b)$.

The least common multiple exists because the set of integers divisible by both $a$ and $b$ is nonempty (as $ab$ belongs to this set, for instance), and every nonempty set of positive integers has a least element (by the well-ordering property, which will be discussed in Section 5.2). Suppose that the prime factorizations of $a$ and $b$ are as before. Then the least common multiple of $a$ and $b$ is given by

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)},$$

where $\max(x, y)$ denotes the maximum of the two numbers $x$ and $y$. This formula is valid because a common multiple of $a$ and $b$ has at least $\max(a_i, b_i)$ factors of $p_i$ in its prime factorization, and the least common multiple has no other prime factors besides those in $a$ and $b$.

**EXAMPLE 15** What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

*Solution:* We have

$$\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,\,4)} 3^{\max(5,\,3)} 7^{\max(2,\,0)} = 2^4 3^5 7^2.$$ ◀

Theorem 5 gives the relationship between the greatest common divisor and least common multiple of two integers. It can be proved using the formulae we have derived for these quantities. The proof of this theorem is left as Exercise 31.

**THEOREM 5** Let $a$ and $b$ be positive integers. Then

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

## The Euclidean Algorithm

Links

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient. The reason is that it is time-consuming to find prime factorizations. We will give a more efficient method of finding the greatest common divisor, called the **Euclidean algorithm**. This algorithm has been known since ancient times. It is named after the ancient Greek mathematician Euclid, who included a description of this algorithm in his book *The Elements*.

Before describing the Euclidean algorithm, we will show how it is used to find $\gcd(91, 287)$. First, divide 287, the larger of the two integers, by 91, the smaller, to obtain

$$287 = 91 \cdot 3 + 14.$$

Any divisor of 91 and 287 must also be a divisor of $287 - 91 \cdot 3 = 14$. Also, any divisor of 91 and 14 must also be a divisor of $287 = 91 \cdot 3 + 14$. Hence, the greatest common divisor of 91 and 287 is the same as the greatest common divisor of 91 and 14. This means that the problem of finding $\gcd(91, 287)$ has been reduced to the problem of finding $\gcd(91, 14)$.

Next, divide 91 by 14 to obtain

$$91 = 14 \cdot 6 + 7.$$

Because any common divisor of 91 and 14 also divides $91 - 14 \cdot 6 = 7$ and any common divisor of 14 and 7 divides 91, it follows that $\gcd(91, 14) = \gcd(14, 7)$.

Continue by dividing 14 by 7, to obtain

$$14 = 7 \cdot 2.$$

Because 7 divides 14, it follows that $\gcd(14, 7) = 7$. Furthermore, because $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$, the original problem has been solved.

We now describe how the Euclidean algorithm works in generality. We will use successive divisions to reduce the problem of finding the greatest common divisor of two positive integers to the same problem with smaller integers, until one of the integers is zero.

The Euclidean algorithm is based on the following result about greatest common divisors and the division algorithm.

Links

EUCLID (325 B.C.E.–265 B.C.E.) Euclid was the author of the most successful mathematics book ever written, *The Elements*, which appeared in over 1000 different editions from ancient to modern times. Little is known about Euclid's life, other than that he taught at the famous academy at Alexandria in Egypt. Apparently, Euclid did not stress applications. When a student asked what he would get by learning geometry, Euclid explained that knowledge was worth acquiring for its own sake and told his servant to give the student a coin "because he must make a profit from what he learns."

**LEMMA 1** Let $a = bq + r$, where $a, b, q$, and $r$ are integers. Then $\gcd(a, b) = \gcd(b, r)$.

*Proof:* If we can show that the common divisors of $a$ and $b$ are the same as the common divisors of $b$ and $r$, we will have shown that $\gcd(a, b) = \gcd(b, r)$, because both pairs must have the same *greatest* common divisor.

So suppose that $d$ divides both $a$ and $b$. Then it follows that $d$ also divides $a - bq = r$ (from Theorem 1 of Section 4.1). Hence, any common divisor of $a$ and $b$ is also a common divisor of $b$ and $r$.

Likewise, suppose that $d$ divides both $b$ and $r$. Then $d$ also divides $bq + r = a$. Hence, any common divisor of $b$ and $r$ is also a common divisor of $a$ and $b$.

Consequently, $\gcd(a, b) = \gcd(b, r)$. ◁

Suppose that $a$ and $b$ are positive integers with $a \ge b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 & \quad 0 \le r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 & \quad 0 \le r_3 < r_2,\\
&\ \ \vdots & \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & \quad 0 \le r_n < r_{n-1},\\
r_{n-1} &= r_n q_n. &
\end{aligned}$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \ge 0$ cannot contain more than $a$ terms. Furthermore, it follows from Lemma 1 that

$$\begin{aligned}
\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots &= \gcd(r_{n-2}, r_{n-1})\\
&= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.
\end{aligned}$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

**EXAMPLE 16** Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

*Solution:* Successive uses of the division algorithm give:

$$\begin{aligned}
662 &= 414 \cdot 1 + 248\\
414 &= 248 \cdot 1 + 166\\
248 &= 166 \cdot 1 + 82\\
166 &= 82 \cdot 2 + 2\\
82 &= 2 \cdot 41.
\end{aligned}$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder. ◀

The Euclidean algorithm is expressed in pseudocode in Algorithm 1.

**ALGORITHM 1 The Euclidean Algorithm.**

**procedure** *gcd*($a, b$: positive integers)
$x := a$
$y := b$
**while** $y \neq 0$
  $r := x$ **mod** $y$
  $x := y$
  $y := r$
**return** $x\{\gcd(a, b) \text{ is } x\}$

In Algorithm 1, the initial values of $x$ and $y$ are $a$ and $b$, respectively. At each stage of the procedure, $x$ is replaced by $y$, and $y$ is replaced by $x$ **mod** $y$, which is the remainder when $x$ is divided by $y$. This process is repeated as long as $y \neq 0$. The algorithm terminates when $y = 0$, and the value of $x$ at that point, the last nonzero remainder in the procedure, is the greatest common divisor of $a$ and $b$.

We will study the time complexity of the Euclidean algorithm in Section 5.3, where we will show that the number of divisions required to find the greatest common divisor of $a$ and $b$, where $a \geq b$, is $O(\log b)$.

## gcds as Linear Combinations

An important result we will use throughout the remainder of this section is that the greatest common divisor of two integers $a$ and $b$ can be expressed in the form

$$sa + tb,$$

where $s$ and $t$ are integers. In other words, $\gcd(a, b)$ can be expressed as a **linear combination** with integer coefficients of $a$ and $b$. For example, $\gcd(6, 14) = 2$, and $2 = (-2) \cdot 6 + 1 \cdot 14$. We state this fact as Theorem 6.

**THEOREM 6** **BÉZOUT'S THEOREM** If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that $\gcd(a, b) = sa + tb$.

Links

ÉTIENNE BÉZOUT (1730–1783) Bézout was born in Nemours, France, where his father was a magistrate. Reading the writings of the great mathematician Leonhard Euler enticed him to become a mathematician. In 1758 he was appointed to a position at the Académie des Sciences in Paris; in 1763 he was appointed examiner of the Gardes de la Marine, where he was assigned the task of writing mathematics textbooks. This assignment led to a four-volume textbook completed in 1767. Bézout is well known for his six-volume comprehensive textbook on mathematics. His textbooks were extremely popular and were studied by many generations of students hoping to enter the École Polytechnique, the famous engineering and science school. His books were translated into English and used in North America, including at Harvard.

His most important original work was published in 1779 in the book *Théorie générale des équations algébriques*, where he introduced important methods for solving simultaneous polynomial equations in many unknowns. The most well-known result in this book is now called *Bézout's theorem*, which in its general form tells us that the number of common points on two plane algebraic curves equals the product of the degrees of these curves. Bézout is also credited with inventing the determinant (which was called the Bézoutian by the great English mathematician James Joseph Sylvester). He was considered to be a kind person with a warm heart, although he had a reserved and somber personality. He was happily married and a father.

**DEFINITION 6** If $a$ and $b$ are positive integers, then integers $s$ and $t$ such that $\gcd(a, b) = sa + tb$ are called *Bézout coefficients* of $a$ and $b$ (after Étienne Bézout, a French mathematician of the eighteenth century). Also, the equation $\gcd(a, b) = sa + tb$ is called *Bézout's identity*.

We will not give a formal proof of Theorem 6 here (see Exercise 36 in Section 5.2 and [Ro10] for proofs). We will provide an example of a general method that can be used to find a linear combination of two integers equal to their greatest common divisor. (In this section, we will assume that a linear combination has integer coefficients.) The method proceeds by working backward through the divisions of the Euclidean algorithm, so this method requires a forward pass and a backward pass through the steps of the Euclidean algorithm. (In the exercises we will describe an algorithm called the **extended Euclidean algorithm**, which can be used to express $\gcd(a, b)$ as a linear combination of $a$ and $b$ using a single pass through the steps of the Euclidean algorithm; see the preamble to Exercise 41.)

**EXAMPLE 17** Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

*Solution:* To show that gcd(252, 198) = 18, the Euclidean algorithm uses these divisions:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

Using the next-to-last division (the third division), we can express gcd(252, 198) = 18 as a linear combination of 54 and 36. We find that

$$18 = 54 - 1 \cdot 36.$$

The second division tells us that

$$36 = 198 - 3 \cdot 54.$$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198. We have

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

The first division tells us that

$$54 = 252 - 1 \cdot 198.$$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

completing the solution. ◀

We will use Theorem 6 to develop several useful results. One of our goals will be to prove the part of the fundamental theorem of arithmetic asserting that a positive integer has at most one prime factorization. We will show that if a positive integer has a factorization into primes, where the primes are written in nondecreasing order, then this factorization is unique.

First, we need to develop some results about divisibility.

**LEMMA 2** If $a$, $b$, and $c$ are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

*Proof:* Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers $s$ and $t$ such that

$$sa + tb = 1.$$

Multiplying both sides of this equation by $c$, we obtain

$$sac + tbc = c.$$

We can now use Theorem 1 of Section 4.1 to show that $a \mid c$. By part (*ii*) of that theorem, $a \mid tbc$. Because $a \mid sac$ and $a \mid tbc$, by part (*i*) of that theorem, we conclude that $a$ divides $sac + tbc$. Because $sac + tbc = c$, we conclude that $a \mid c$, completing the proof. ◁

We will use the following generalization of Lemma 2 in the proof of uniqueness of prime factorizations. (The proof of Lemma 3 is left as Exercise 64 in Section 5.1, because it can be most easily carried out using the method of mathematical induction, covered in that section.)

**LEMMA 3** If $p$ is a prime and $p \mid a_1 a_2 \cdots a_n$, where each $a_i$ is an integer, then $p \mid a_i$ for some $i$.

We can now show that a factorization of an integer into primes is unique. That is, we will show that every integer can be written as the product of primes in nondecreasing order in at most one way. This is part of the fundamental theorem of arithmetic. We will prove the other part, that every integer has a factorization into primes, in Section 5.2.

*Proof (of the uniqueness of the prime factorization of a positive integer):* We will use a proof by contradiction. Suppose that the positive integer $n$ can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, each $p_i$ and $q_j$ are primes such that $p_1 \le p_2 \le \cdots \le p_s$ and $q_1 \le q_2 \le \cdots \le q_t$.

When we remove all common primes from the two factorizations, we have

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v},$$

where no prime occurs on both sides of this equation and $u$ and $v$ are positive integers. By Lemma 3 it follows that $p_{i_1}$ divides $q_{j_k}$ for some $k$. Because no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of $n$ into primes in nondecreasing order. ◁

Lemma 2 can also be used to prove a result about dividing both sides of a congruence by the same integer. We have shown (Theorem 5 in Section 4.1) that we can multiply both sides of a congruence by the same integer. However, dividing both sides of a congruence by an integer does not always produce a valid congruence, as Example 18 shows.

**EXAMPLE 18** The congruence $14 \equiv 8 \pmod{6}$ holds, but both sides of this congruence cannot be divided by 2 to produce a valid congruence because $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$. ◀

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

**THEOREM 7** Let $m$ be a positive integer and let $a$, $b$, and $c$ be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

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

## Exercises

**1.** Determine whether each of these integers is prime.
**a)** 21 **b)** 29
**c)** 71 **d)** 97
**e)** 111 **f)** 143

**2.** Determine whether each of these integers is prime.
**a)** 19 **b)** 27
**c)** 93 **d)** 101
**e)** 107 **f)** 113

**3.** Find the prime factorization of each of these integers.
**a)** 88 **b)** 126 **c)** 729
**d)** 1001 **e)** 1111 **f)** 909,090

**4.** Find the prime factorization of each of these integers.
**a)** 39 **b)** 81 **c)** 101
**d)** 143 **e)** 289 **f)** 899

**5.** Find the prime factorization of 10!.

***6.** How many zeros are there at the end of 100!?

**7.** Express in pseudocode the trial division algorithm for determining whether an integer is prime.

**8.** Express in pseudocode the algorithm described in the text for finding the prime factorization of an integer.

**9.** Show that if $a^m + 1$ is composite if $a$ and $m$ are integers greater than 1 and $m$ is odd. [*Hint:* Show that $x + 1$ is a factor of the polynomial $x^m + 1$ if $m$ is odd.]

**10.** Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer $n$. [*Hint:* First show that the polynomial identity $x^m + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + \cdots - x^k + 1)$ holds, where $m = kt$ and $t$ is odd.]

***11.** Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number $x$ that cannot be written as the ratio of two integers.

**12.** Prove that for every positive integer $n$, there are $n$ consecutive composite integers. [*Hint:* Consider the $n$ consecutive integers starting with $(n + 1)! + 2$.]

***13.** Prove or disprove that there are three consecutive odd positive integers that are primes, that is, odd primes of the form $p$, $p + 2$, and $p + 4$.

**14.** Which positive integers less than 12 are relatively prime to 12?

**15.** Which positive integers less than 30 are relatively prime to 30?

**16.** Determine whether the integers in each of these sets are pairwise relatively prime.
**a)** 21, 34, 55 **b)** 14, 17, 85
**c)** 25, 41, 49, 64 **d)** 17, 18, 19, 23

**17.** Determine whether the integers in each of these sets are pairwise relatively prime.
**a)** 11, 15, 19 **b)** 14, 15, 21
**c)** 12, 17, 31, 37 **d)** 7, 8, 9, 11

**18.** We call a positive integer **perfect** if it equals the sum of its positive divisors other than itself.
**a)** Show that 6 and 28 are perfect.
**b)** Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

**19.** Show that if $2^n - 1$ is prime, then $n$ is prime. [*Hint:* Use the identity $2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$.]

**20.** Determine whether each of these integers is prime, verifying some of Mersenne's claims.
**a)** $2^7 - 1$ **b)** $2^9 - 1$
**c)** $2^{11} - 1$ **d)** $2^{13} - 1$

The value of the **Euler $\phi$-function** at the positive integer $n$ is defined to be the number of positive integers less than or equal to $n$ that are relatively prime to $n$. [*Note:* $\phi$ is the Greek letter phi.]

**21.** Find these values of the Euler $\phi$-function.
**a)** $\phi(4)$. **b)** $\phi(10)$. **c)** $\phi(13)$.

**22.** Show that $n$ is prime if and only if $\phi(n) = n - 1$.

**23.** What is the value of $\phi(p^k)$ when $p$ is prime and $k$ is a positive integer?

**24.** What are the greatest common divisors of these pairs of integers?
**a)** $2^2 \cdot 3^3 \cdot 5^5$, $2^5 \cdot 3^3 \cdot 5^2$
**b)** $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

**c)** 17, $17^{17}$ **d)** $2^2 \cdot 7, 5^3 \cdot 13$
**e)** 0, 5 **f)** $2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7$

**25.** What are the greatest common divisors of these pairs of integers?

**a)** $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$
**b)** $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
**c)** $23^{31}, 23^{17}$
**d)** $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
**e)** $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
**f)** 1111, 0

**26.** What is the least common multiple of each pair in Exercise 24?

**27.** What is the least common multiple of each pair in Exercise 25?

**28.** Find gcd(1000, 625) and lcm(1000, 625) and verify that $\gcd(1000, 625) \cdot \text{lcm}(1000, 625) = 1000 \cdot 625$.

**29.** Find gcd(92928, 123552) and lcm(92928, 123552), and verify that gcd(92928, 123552) · lcm(92928, 123552) = 92928 · 123552. [*Hint:* First find the prime factorizations of 92928 and 123552.]

**30.** If the product of two integers is $2^7 3^8 5^2 7^{11}$ and their greatest common divisor is $2^3 3^4 5$, what is their least common multiple?

**31.** Show that if $a$ and $b$ are positive integers, then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$. [*Hint:* Use the prime factorizations of $a$ and $b$ and the formulae for $\gcd(a, b)$ and $\text{lcm}(a, b)$ in terms of these factorizations.]

**32.** Use the Euclidean algorithm to find

**a)** gcd(1, 5). **b)** gcd(100, 101).
**c)** gcd(123, 277). **d)** gcd(1529, 14039).
**e)** gcd(1529, 14038). **f)** gcd(11111, 111111).

**33.** Use the Euclidean algorithm to find

**a)** gcd(12, 18). **b)** gcd(111, 201).
**c)** gcd(1001, 1331). **d)** gcd(12345, 54321).
**e)** gcd(1000, 5040). **f)** gcd(9888, 6060).

**34.** How many divisions are required to find gcd(21, 34) using the Euclidean algorithm?

**35.** How many divisions are required to find gcd(34, 55) using the Euclidean algorithm?

***36.** Show that if $a$ and $b$ are both positive integers, then $(2^a - 1) \mathbf{mod} (2^b - 1) = 2^{a \mathbf{mod} b} - 1$.

***37.** Use Exercise 36 to show that if $a$ and $b$ are positive integers, then $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. [*Hint:* Show that the remainders obtained when the Euclidean algorithm is used to compute $\gcd(2^a - 1, 2^b - 1)$ are of the form $2^r - 1$, where $r$ is a remainder arising when the Euclidean algorithm is used to find $\gcd(a, b)$.]

**38.** Use Exercise 37 to show that the integers $2^{35} - 1$, $2^{34} - 1$, $2^{33} - 1$, $2^{31} - 1$, $2^{29} - 1$, and $2^{23} - 1$ are pairwise relatively prime.

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

**a)** 10, 11 **b)** 21, 44 **c)** 36, 48
**d)** 34, 55 **e)** 117, 213 **f)** 0, 223
**g)** 123, 2347 **h)** 3454, 4666 **i)** 9999, 11111

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

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

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

**41.** Use the extended Euclidean algorithm to express gcd(26, 91) as a linear combination of 26 and 91.

**42.** Use the extended Euclidean algorithm to express gcd(252, 356) as a linear combination of 252 and 356.

**43.** Use the extended Euclidean algorithm to express gcd(144, 89) as a linear combination of 144 and 89.

**44.** Use the extended Euclidean algorithm to express gcd(1001, 100001) as a linear combination of 1001 and 100001.

**45.** Describe the extended Euclidean algorithm using pseudocode.

**46.** Find the smallest positive integer with exactly $n$ different positive factors when $n$ is

**a)** 3. **b)** 4. **c)** 5.
**d)** 6. **e)** 10.

**47.** Can you find a formula or rule for the $n$th term of a sequence related to the prime numbers or prime factorizations so that the initial terms of the sequence have these values?

**a)** 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, ...
**b)** 1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, ...
**c)** 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, ...
**d)** 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, ...
**e)** 1, 2, 3, 3, 5, 5, 7, 7, 7, 7, 11, 11, 13, 13, ...
**f)** 1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, ...

**48.** Can you find a formula or rule for the $n$th term of a sequence related to the prime numbers or prime factorizations so that the initial terms of the sequence have these values?

**a)** 2, 2, 3, 5, 5, 7, 7, 11, 11, 11, 11, 13, 13, ...
**b)** 0, 1, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 6, 6, ...
**c)** 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, ...
**d)** 1, −1, −1, 0, −1, 1, −1, 0, 0, 1, −1, 0, −1, 1, 1, ...
**e)** 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, ...
**f)** 4, 9, 25, 49, 121, 169, 289, 361, 529, 841, 961, 1369, ...

**49.** Prove that the product of any three consecutive integers is divisible by 6.

**50.** Show that if $a$, $b$, and $m$ are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

***51.** Prove or disprove that $n^2 - 79n + 1601$ is prime whenever $n$ is a positive integer.

**52.** Prove or disprove that $p_1 p_2 \cdots p_n + 1$ is prime for every positive integer $n$, where $p_1, p_2, \ldots, p_n$ are the $n$ smallest prime numbers.

**53.** Show that there is a composite integer in every arithmetic progression $ak + b$, $k = 1, 2, \ldots$ where $a$ and $b$ are positive integers.

**54.** Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form $3k + 2$, where $k$ is a nonnegative integer. [*Hint:* Suppose that there are only finitely many such primes $q_1, q_2, \ldots, q_n$, and consider the number $3q_1q_2 \cdots q_n - 1$.]

**55.** Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form $4k + 3$, where $k$ is a nonnegative integer. [*Hint:* Suppose that there are only finitely many such primes $q_1, q_2, \ldots, q_n$, and consider the number $4q_1q_2 \cdots q_n - 1$.]

***56.** Prove that the set of positive rational numbers is countable by setting up a function that assigns to a rational number $p/q$ with $\gcd(p, q) = 1$ the base 11 number formed by the decimal representation of $p$ followed by the base 11 digit A, which corresponds to the decimal number 10, followed by the decimal representation of $q$.

***57.** Prove that the set of positive rational numbers is countable by showing that the function $K$ is a one-to-one correspondence between the set of positive rational numbers and the set of positive integers if $K(m/n) = p_1^{2a_1} p_2^{2a_2} \cdot \cdots \cdot p_s^{2a_s} q_1^{2b_1-1} q_2^{2b_2-1} \cdot \cdots \cdot q_t^{2b_t-1}$, where $\gcd(m, n) = 1$ and the prime-power factorizations of $m$ and $n$ are $m = p_1^{a_1} p_2^{a_2} \cdot \cdots \cdot p_s^{a_s}$ and $n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$.

# 4.4 Solving Congruences

## Introduction

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

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

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

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