2.4 The Integers and Division

INTRODUCTION

The part of discrete mathematics involving the integers and their properties belongs to the branch of mathematics called **number theory.** This section is the beginning of a three-section introduction to number theory. In this section we will review some basic concepts of number theory, including divisibility, greatest common divisors, and modular arithmetic. In Section 2.5 we will describe several important algorithms from number theory, tying together the material in Sections 2.1 and 2.3 on algorithms and their complexity with the notions introduced in this section. For example, we will introduce algorithms for finding the greatest common divisor of two positive integers and for performing computer arithmetic using binary expansions. Finally, in Section 2.6, we will continue our study of number theory by introducing some important results and their applications to computer arithmetic and cryptology, the study of secret messages.

The ideas that we will develop in this section are based on the notion of divisibility. One important concept based on divisibility is that of a prime number. A prime is an integer greater than 1 that is divisible only by 1 and by itself. Determining whether an integer is prime is important in applications to cryptology. An important theorem from number theory, the Fundamental Theorem of Arithmetic, asserts that every positive integer can be written uniquely as the product of prime numbers. Factoring integers into their prime factors is important in cryptology. Division of an integer by a positive integer produces a quotient and a remainder. Working with these remainders leads to modular arithmetic, which is used throughout computer science. We will discuss three applications of modular arithmetic in this section: generating pseudorandom numbers, assigning computer memory locations to files, and encrypting and decrypting 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 the following definition.

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 $b = ac$. When a divides b we say that a is a *factor* 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 $3 \mid 12$.

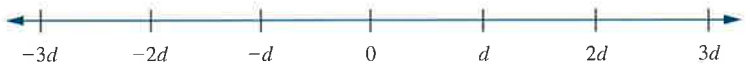

FIGURE 1 **Integers Divisible by the Positive Integer *d*.**

Solution: It follows that $3 \nmid 7$, since $7/3$ is not an integer. On the other hand, $3 \mid 12$ since $12/3 = 4$. ◀

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. Then

1. if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
2. if $a \mid b$, then $a \mid bc$ for all integers c;
3. if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: To prove (*1*) 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,

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

Therefore, a divides $b + c$. This establishes part (*1*) of the theorem. The proofs of parts (*2*) and (*3*) are left as exercises for the reader. ◁

Theorem 1 has this useful consequence.

COROLLARY 1

If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Proof: By part (*2*) of Theorem 1 it follows that $a \mid mb$ and $a \mid nc$ whenever m and n are integers. By part (*1*) of Theorem 1 it follows that $a \mid mb + nc$. ◁

PRIMES

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

DEFINITION 2 A positive 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 3 The integer 7 is prime since its only positive factors are 1 and 7, whereas the integer 9 is composite since it is divisible by 3. ◀

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. In Section 6.6 we introduce a procedure, known as the **sieve of Eratosthenes,** which can be used to find all the primes not exceeding an integer n.

The primes are the building blocks of positive integers, as the Fundamental Theorem of Arithmetic shows. The proof will be given in Section 3.3.

THEOREM 2 **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every positive 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 4 gives some prime factorizations of integers.

EXAMPLE 4 The prime factorizations of 100, 641, 999, and 1024 are given by

Extra Examples

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$
$$641 = 641,$$
$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$
$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$ ◀

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

Proof: If n is composite, it has a factor a with $1 < a < n$. Hence, $n = ab$, where both a and b are positive integers greater than 1. We see that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, since otherwise $ab > \sqrt{n} \cdot \sqrt{n} = n$. Hence, 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. In either case, n has a prime divisor less than or equal to $\sqrt{n}$. ◁

From Theorem 3, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. In the following example this observation is used to show that 101 is prime.

EXAMPLE 5 Show that 101 is prime.

Solution: The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Since 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. ◀

Since 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 6.

EXAMPLE 6 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, since $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Since 13 is prime, the procedure is completed. It follows that the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$. ◀

Links

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 2.6.

THE INFINITUDE OF PRIMES It has long been known that there are infinitely many primes. We will prove this fact using a proof given by Euclid in his famous mathematics text, the *Elements*.

THEOREM 4 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 $Q - p_1 p_2 \cdots p_n = 1$. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes. (Note that in this proof we do *not* state that Q is prime!) ◁

Since 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. 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 certain special forms anywhere near as quickly to determine whether they are prime.

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

Progress in finding Mersenne primes has been steady since computers were invented. As of mid-2002, 39 Mersenne primes were known, with eight found since 1990. The largest Mersenne prime known (as of mid-2002) is $2^{13,466,917} - 1$, a number with over four million digits, which was shown to be prime in late 2001. A communal effort, the Great Internet Mersenne Prime Search (GIMPS), has been organized to look for new Mersenne primes. 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.

THE DISTRIBUTION OF PRIMES Theorem 4 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 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 5.

THEOREM 5

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.)

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 considered themselves the least religious order). 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.

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 Valleé-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 of a certain size 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 x is prime are approximately $(x/\ln x)/x = 1/\ln x$. 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 3 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. However, even though powerful new factorization methods have been developed in the same time frame, factoring large numbers remains extraordinarily more time consuming. 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.

Links

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 6

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 $a = dq + r$.

Remark: Theorem 6 is not really an algorithm. (Why not?) Nevertheless, we use its traditional name.

DEFINITION 3

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:

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

Examples 8 and 9 illustrate the division algorithm.

EXAMPLE 8 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 9 What are the quotient and remainder when -11 is divided by 3?

Extra Examples

Solution: We have

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

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

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

since $r = -2$ 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.

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 4 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 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 the following examples. 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 $\gcd(17, 22) = 1$. ◀

Since it is often important to specify that two integers have no common positive divisor other than 1, we have the following definition.

DEFINITION 5 The integers a and b are *relatively prime* if their greatest common divisor is 1.

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

Since 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 6.

DEFINITION 6 The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

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

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

Another way to find the greatest common divisor of two integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the integers a and b, neither equal to zero, are

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

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, since 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 Since 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 7 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 $\text{lcm}(a, b)$.

The least common multiple exists because the set of integers divisible by both a and b is nonempty, and every nonempty set of positive integers has a least element (by the well-ordering property, which will be discussed in Section 3.3). Suppose that the prime factorizations of a and b are as before. Then the least common multiple of a and b is given by

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

where $\max(x, y)$ denotes the maximum of the two numbers x and y. This formula is valid since 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

$$\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2. \quad \blacktriangleleft$$

The following theorem 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 an exercise for the reader.

THEOREM 7 Let a and b be positive integers. Then

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

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. Since we are often interested only in remainders, we have special notations for them.

We have a notation to indicate that two integers have the same remainder when they are divided by the positive integer m.

DEFINITION 8 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. If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

The connection between the notations used when working with remainders is made clear in Theorem 8.

THEOREM 8 Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

The proof of Theorem 8 is left as Exercises 21 and 22 at the end of this section.

EXAMPLE 16 Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution: Since 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$. However, since $24 - 14 = 10$ 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 9 provides a useful way to work with congruences.

THEOREM 9 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 $a \equiv b \pmod{m}$, then $m \mid (a - b)$. 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 7 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 10 shows how congruences work with respect to addition and multiplication.

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 10

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

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

Proof: Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, 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,

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

EXAMPLE 17 Since $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 10 that

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

and that

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

APPLICATIONS OF CONGRUENCES

Number theory has applications to a wide range of areas. We will introduce three applications in this section: the use of congruences to assign memory locations to computer files, the generation of pseudorandom numbers, and cryptosystems based on modular arithmetic.

EXAMPLE 18 **Hashing Functions** The central computer at your school maintains records for each student. How can memory locations be assigned so that student records can be retrieved quickly? The solution to this problem is to use a suitably chosen **hashing function.** Records are identified using a **key,** which uniquely identifies each student's records. For instance, student records are often identified using the Social Security number of the student as the key. A hashing function h assigns memory location $h(k)$ to the record that has k as its key.

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

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

where m is the number of available memory locations.

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

For example, when $m = 111$, the record of the student with Social Security number 064212848 is assigned to memory location 14, since

$$h(064212848) = 064212848 \textbf{ mod } 111 = 14.$$

Similarly, since

$$h(037149212) = 037149212 \textbf{ mod } 111 = 65,$$

the record of the student with Social Security number 037149212 is assigned to memory location 65.

Since a hashing function is not one-to-one (since there are more possible keys than memory locations), more than one file may be assigned to a memory location. When this happens, we say that a **collision** occurs. One way to resolve a collision is to assign the first free location following the occupied memory location assigned by the hashing function. For example, after making the two earlier assignments, we assign location 15 to the record of the student with the Social Security number 107405723. To see this, first note that $h(k)$ maps this Social Security number to location 14, since

$$h(107405723) = 107405723 \textbf{ mod } 111 = 14,$$

but this location is already occupied (by the file of the student with Social Security number 064212848). However, memory location 15, the first location following memory location 14, is free.

There are many more sophisticated ways to resolve collisions that are more efficient than the simple method we have described. These are discussed in the references on hashing functions given at the end of the book. ◀

EXAMPLE 19 **Pseudorandom Numbers** Randomly chosen numbers are often needed for computer simulations. Different methods have been devised for generating numbers that have properties of randomly chosen numbers. Because numbers generated by systematic methods are not truly random, they are called **pseudorandom numbers.**

The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method.** We choose four integers: the **modulus** m, **multiplier** a, **increment** c, and **seed** x_0, with $2 \leq a < m$, $0 \leq c < m$, and $0 \leq x_0 < m$. We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the congruence

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

(This is an example of a recursive definition, discussed in Section 3.4. In that section we will show that such sequences are well defined.)

Many computer experiments require the generation of pseudorandom numbers between 0 and 1. To generate such numbers, we divide numbers generated with a linear congruential generator by the modulus: that is, we use the numbers x_n/m.

For instance, the sequence of pseudorandom numbers generated by choosing $m = 9$, $a = 7$, $c = 4$, and $x_0 = 3$, can be found as follows:

$$x_1 = 7x_0 + 4 = 7 \cdot 3 + 4 = 25 \textbf{ mod } 9 = 7,$$
$$x_2 = 7x_1 + 4 = 7 \cdot 7 + 4 = 53 \textbf{ mod } 9 = 8,$$
$$x_3 = 7x_2 + 4 = 7 \cdot 8 + 4 = 60 \textbf{ mod } 9 = 6,$$
$$x_4 = 7x_3 + 4 = 7 \cdot 6 + 4 = 46 \textbf{ mod } 9 = 1,$$

$$x_5 = 7x_4 + 4 = 7 \cdot 1 + 4 = 11 \bmod 9 = 2,$$
$$x_6 = 7x_5 + 4 = 7 \cdot 2 + 4 = 18 \bmod 9 = 0,$$
$$x_7 = 7x_6 + 4 = 7 \cdot 0 + 4 = 4 \bmod 9 = 4,$$
$$x_8 = 7x_7 + 4 = 7 \cdot 4 + 4 = 32 \bmod 9 = 5,$$
$$x_9 = 7x_8 + 4 = 7 \cdot 5 + 4 = 39 \bmod 9 = 3.$$

Since $x_9 = x_0$ and since each term depends only on the previous term, this sequence is generated:

$$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots.$$

This sequence contains nine different numbers before repeating.

Most computers do use linear congruential generators to generate pseudorandom numbers. Often, a linear congruential generator with increment $c = 0$ is used. Such a generator is called a **pure multiplicative generator.** For example, the pure multiplicative generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ is widely used. With these values, it can be shown that $2^{31} - 2$ numbers are generated before repetition begins. ◀

CRYPTOLOGY

Congruences have many applications to discrete mathematics and computer science. Discussions of these applications can be found in the suggested readings given at the end of the book. One of the most important applications of congruences involves **cryptology,** which is the study of secret messages. One of the earliest known uses of cryptology was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three). For instance, using this scheme the letter B is sent to E and the letter X is sent to A. This is an example of **encryption,** that is, the process of making a message secret.

To express Caesar's encryption process mathematically, first replace each letter by an integer from 0 to 25, based on its position in the alphabet. For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer p, $p \leq 25$, the integer $f(p)$ in the set $\{0, 1, 2, \ldots, 25\}$ with

$$f(p) = (p + 3) \bmod 26.$$

In the encrypted version of the message, the letter represented by p is replaced with the letter represented by $(p + 3) \bmod 26$.

EXAMPLE 20 What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution: First replace the letters in the message with numbers. This produces

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$. This gives

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN." ◀

To recover the original message from a secret message encrypted by the Caesar cipher, the function f^{-1}, the inverse of f, is used. Note that the function f^{-1} sends an integer p from $\{0, 1, 2, \ldots, 25\}$ to $f^{-1}(p) = (p - 3) \bmod 26$. In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet. The process of determining the original message from the encrypted message is called **decryption.**

There are various ways to generalize the Caesar cipher. For example, instead of shifting each letter by 3, we can shift each letter by k, so that

$$f(p) = (p + k) \bmod 26.$$

Such a cipher is called a **shift cipher.** Note that decryption can be carried out using

$$f^{-1}(p) = (p - k) \bmod 26.$$

Obviously, Caesar's method and shift ciphers do not provide a high level of security. There are various ways to enhance this method. One approach that slightly enhances the security is to use a function of the form

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen such that f is a bijection. (Such a mapping is called an *affine transformation*.) This provides a number of possible encryption systems. The use of one of these systems is illustrated in the following example.

EXAMPLE 21 What letter replaces the letter K when the function $f(p) = (7p + 3) \bmod 26$ is used for encryption?

Solution: First, note that 10 represents K. Then, using the encryption function specified, it follows that $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$. Since 21 represents V, K is replaced by V in the encrypted message. ◀

Links

Caesar's encryption method, and the generalization of this method, proceed by replacing each letter of the alphabet by another letter in the alphabet. Encryption methods of this kind are vulnerable to attacks based on the frequency of occurrence of letters in the message. More sophisticated encryption methods are based on replacing blocks of letters with other blocks of letters. There are a number of techniques based on modular arithmetic for encrypting blocks of letters. A discussion of these can be found in the suggested readings listed at the end of the book.

Exercises

1. Does 17 divide each of these numbers?
   a) 68 **b)** 84 **c)** 357 **d)** 1001
2. Show that if a is an integer other than 0, then
   a) 1 divides a. **b)** a divides 0.
3. Show that part (2) of Theorem 1 is true.
4. Show that part (3) 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 such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.
7. Show that if a, b, and c are integers such that $ac \mid bc$, then $a \mid b$.
8. Are these integers primes?
   a) 19 **b)** 27
   c) 93 **d)** 101
   e) 107 **f)** 113

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. Find the prime factorization of each of these integers.

a) 88 **b)** 126 **c)** 729
d) 1001 **e)** 1111 **f)** 909,090

12. Find the prime factorization of each of these integers.

a) 39 **b)** 81 **c)** 101
d) 143 **e)** 289 **f)** 899

13. Find the prime factorization of 10!.

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

***15.** 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.

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

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

18. 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

19. 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

20. 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.

21. Let m be a positive integer. Show that $a \equiv b$ (**mod** m) if a **mod** $m = b$ **mod** m.

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

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

24. 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)** $2^{13} - 1$

25. The value of the **Euler ϕ-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:* ϕ is the Greek letter phi.) Find

a) $\phi(4)$. **b)** $\phi(10)$. **c)** $\phi(13)$.

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

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

28. 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)** $2 \cdot 3 \cdot 5 \cdot 7$, $2 \cdot 3 \cdot 5 \cdot 7$

29. 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

30. What is the least common multiple of each pair in Exercise 28?

31. What is the least common multiple of each pair in Exercise 29?

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

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

34. Show that if a is an integer and d is a positive 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.

35. 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.

36. Evaluate these quantities.

a) −17 **mod** 2 **b)** 144 **mod** 7
c) −101 **mod** 13 **d)** 199 **mod** 19

37. Evaluate these quantities.

a) 13 **mod** 3 **b)** −97 **mod** 11
c) 155 **mod** 19 **d)** −221 **mod** 23

38. List five integers that are congruent to 4 modulo 12.

39. Decide whether each of these integers is congruent to 5 modulo 17.

a) 80 **b)** 103
c) −29 **d)** −122

40. 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?

41. 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.]

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

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

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

45. Show that $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, does not necessarily imply that $a \equiv b \pmod{m}$.

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

47. Show that if a, b, k, and m are integers such that $k \geq 1$, $m \geq 2$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ whenever k is a positive integer.

48. Which memory locations are assigned by the hashing function $h(k) = k$ **mod** 101 to the records of students with these Social Security numbers?

a) 104578690 **b)** 432222187
c) 372201919 **d)** 501338753

49. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function $h(k) = k$ **mod** 31, where k is the number formed from the first three digits on a visitor's license plate.

a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates?

317, 918, 007, 100, 111, 310

b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

50. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 1)$ **mod** 7 with seed $x_0 = 3$?

51. What sequence of pseudorandom numbers is generated using the pure multiplicative generator $x_{n+1} = 3x_n$ **mod** 11 with seed $x_0 = 2$?

52. Write an algorithm in pseudocode for generating a sequence of pseudorandom numbers using a linear congruential generator.

53. Encrypt the message "DO NOT PASS GO" by translating the letters into numbers, applying the encryption function given, and then translating the numbers back into letters.

a) $f(p) = (p + 3)$ **mod** 26 (the Caesar cipher)
b) $f(p) = (p + 13)$ **mod** 26
c) $f(p) = (3p + 7)$ **mod** 26

54. Decrypt these messages encrypted using the Caesar cipher.

a) EOXH MHDQV
b) WHVW WRGDB
c) HDW GLP VXP

Books are identified by an **International Standard Book Number (ISBN),** a 10-digit code $x_1 x_2 \ldots x_{10}$, assigned by the publisher. These 10 digits consist of blocks identifying the language, the publisher, the number assigned to the book by its publishing company, and finally, a 1-digit check digit that is either a digit or the letter X (used to represent 10). This check digit is selected so that $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$ and is used to detect errors in individual digits and transposition of digits.

55. The first nine digits of the ISBN of the third edition of this book are 0-07-053965. What is the check digit for this book?

56. The ISBN of *Elementary Number Theory and Its Applications,* 3rd ed., is 0-201-57Q89-1, where Q is a digit. Find the value of Q.

57. Determine whether the check digit of the ISBN for this textbook was computed correctly by the publisher.

58. Find the smallest positive integer with exactly n different factors when n is

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

59. Can you find a formula or rule for the nth 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, ...

60. Can you find a formula or rule for the nth 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, ...