3 Primes and Greatest Common Divisors

This chapter introduces a central concept of number theory, namely, that of a prime number. A prime is an integer with precisely two positive integer divisors. Prime numbers were studied extensively by the ancient Greeks, who discovered many of their basic properties. In the past three centuries, mathematicians have devoted countless hours to exploring the world of primes. They have discovered many fascinating properties, formulated diverse conjectures, and proved interesting and surprising results. Research into questions involving primes continues today, partly driven by the importance of primes in modern cryptography. Open questions about primes stimulate new research. There are also tens of thousands of people trying to enter the record books by finding the largest prime yet known.

In this chapter, we will show that there are infinitely many primes. The proof we will give dates back to ancient times. We will also show how to find all the primes not exceeding a given integer, using the sieve of Eratosthenes, also dating back to antiquity. We will discuss the distribution of primes, and state the famous prime number theorem that was proved at the end of the nineteenth century. This theorem provides an accurate estimate for the number of primes not exceeding a given integer. Many questions about primes remain open despite attention from mathematicians over hundreds of years; we will discuss a selection of such problems, including two of the best known, the twin prime conjecture and Goldbach's conjecture.

This chapter also shows that every positive integer can be written uniquely as the product of primes (when the primes are written in increasing order of size). This result is known as the *fundamental theorem of arithmetic*. To prove this theorem, we will use the concept of the greatest common divisor of two integers. We will establish many important properties of the greatest common divisor in this chapter, such as the fact that it is the smallest positive linear combination of these integers. We will describe the Euclidean algorithm that can be used for finding the greatest common divisor of two integers, and analyze its computational complexity. We will discuss methods used to find the factorization of integers into products of primes, and discuss the complexity of these methods. Numbers of special form are often studied in number theory; in this chapter, we will introduce the Fermat numbers, which are integers of the form $2^{2^n} + 1$. (Fermat conjectured that they are all prime but this turns out not to be true.)

Finally, we will introduce the concept of a diophantine equation, which is an equation where only solutions in integers are sought. We will show how greatest common divisors can be used to help solve linear diophantine equations. Unlike many other diophantine equations, linear diophantine equations can be solved easily and systematically.

3.1 Prime Numbers

The positive integer 1 has just one positive divisor. Every other positive integer has at least two positive divisors, because it is divisible by 1 and by itself. Integers with exactly two positive divisors are of great importance in number theory; they are called *primes.*

Definition. A *prime* is an integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example 3.1. The integers 2, 3, 5, 13, 101, and 163 are primes. ◀

Definition. An integer greater than 1 that is not prime is called *composite.*

Example 3.2. The integers $4 = 2 \cdot 2$, $8 = 4 \cdot 2$, $33 = 3 \cdot 11$, $111 = 3 \cdot 37$, and $1001 = 7 \cdot 11 \cdot 13$ are composite. ◀

The primes are the multiplicative building blocks of the integers. Later, we will show that every positive integer can be written uniquely as the product of primes.

In this section, we will discuss the distribution of prime numbers among the set of positive integers, and prove some elementary properties about this distribution. We will also discuss more powerful results about the distribution of primes. The theorems we will introduce include some of the most famous results in number theory.

You can find all primes less than 10,000 in Table E.1 at the end of the book.

The Infinitude of Primes

We start by showing that there are infinitely many primes, for which the following lemma is needed.

Lemma 3.1. Every integer greater than 1 has a prime divisor.

Proof. We prove the lemma by contradiction; we assume that there is a positive integer greater than 1 having no prime divisors. Then, since the set of positive integers greater than 1 with no prime divisors is nonempty, the well-ordering property tells us that there is a least positive integer n greater than 1 with no prime divisors. Because n has no prime divisors and n divides n, we see that n is not prime. Hence, we can write $n = ab$ with $1 < a < n$ and $1 < b < n$. Because $a < n$, a must have a prime divisor. By Theorem 1.8, any divisor of a is also a divisor of n, so n must have a prime divisor, contradicting the fact that n has no prime divisors. We can conclude that every positive integer greater than 1 has at least one prime divisor. ■

We now show that there are infinitely many primes, a wondrous result known by the ancient Greeks. This is one of the key theorems in number theory that can be proved in a variety of ways. The proof we will provide was presented by Euclid in his book the *Elements* (Book IX, 20). This simple yet elegant proof is considered by many to be particularly beautiful. It is not surprising that the very first proof found in the book *Proofs*

from THE BOOK [AiZi10], a collection of particularly insightful and clever proofs, begins with this proof found in Euclid. Moreover, this book presents six quite different proofs of the infinitude of primes. (Here, *THE BOOK* refers to the imagined collection of perfect proofs that Paul Erdős claimed is maintained by God.) We will introduce a variety of different proofs that there are infinitely many primes later in this chapter. (See Exercise 8 at the end of this section, the exercise sets in Sections 3.3 and 3.5, and Section 3.6.)

Theorem 3.1. There are infinitely many primes.

Proof. Suppose that there are only finitely many primes, $p_1, p_2, \ldots p_n$, where n is a positive integer. Consider the integer Q_n, obtained by multiplying these primes together and adding one, that is,

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

By Lemma 3.1, Q has at least one prime divisor, say, q. We obtain a contradiction by showing that q is not one of the primes listed. (These supposedly formed a complete list of all primes.) If $q = p_j$ for some integer j with $1 \leq j \leq n$, then since $Q_n - p_1 p_2 \cdots p_n = 1$, because q divides both terms on the left-hand side of this equation, by Theorem 1.9 it follows that $q \mid 1$. This is impossible because no prime divides 1. Consequently, q must be a prime we have not listed. This contradiction shows that there are infinity many primes. ∎

The proof of Theorem 3.1 is nonconstructive because the integer we have constructed in the proof, Q_n, which is one more than the product of the first n primes, may or may not be prime (see Exercise 11). Consequently, in the proof we have not found a new prime, but we know that one exists.

Finding Primes In later chapters, we will be interested in finding and using extremely large primes. Tests distinguishing between primes and composite integers will be crucial; such tests are called *primality tests*. The most basic primality test is *trial division,* which tells us that the integer n is prime if and only if it is not divisible by any prime not exceeding $\sqrt{n}$. We now prove that this test can be used to determine whether n is prime.

Theorem 3.2. If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.

Proof. Because n is composite, we can write $n = ab$, where a and b are integers with $1 < a \leq b < n$. We must have $a \leq \sqrt{n}$, since otherwise $b \geq a > \sqrt{n}$ and $ab > \sqrt{n} \cdot \sqrt{n} = n$. Now, by Lemma 3.1, a must have a prime divisor, which by Theorem 1.8 is also a divisor of n and which is clearly less than or equal to $\sqrt{n}$. ∎

We can use Theorem 3.2 to find all the primes less than or equal to a given positive integer n. This procedure is called the *sieve of Eratosthenes,* since it was invented by the ancient Greek mathematician *Eratosthenes*. We illustrate its use in Figure 3.1 by finding all primes less than 100. We first note that every composite integer less than 100 must have a prime factor less than $\sqrt{100} = 10$. Because the only primes less than 10 are 2, 3, 5, and 7, we only need to check each integer less than 100 for divisibility by these primes. We first cross out, with a horizontal line (—), all multiples of 2 greater than 2.

Next, we cross out with a slash (/) those integers remaining that are multiples of 3, other than 3 itself. Then all multiples of 5, other than 5, that remain are crossed out with a backslash (\). Finally, all multiples of 7, other than 7, that are left are crossed out with a vertical stroke (|). All remaining integers (other than 1, which we cross out using an ×) must be prime (and are shown in boldface in the figure).

×	**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~~

Figure 3.1 *Using the sieve of Eratosthenes to find the primes less than 100.*

Although the sieve of Eratosthenes produces all primes less than or equal to a fixed integer, to determine in this manner whether a particular integer n is prime it is necessary to check n for divisibility by all primes not exceeding $\sqrt{n}$. This is quite inefficient; later, we will give better methods for deciding whether or not an integer is prime.

We now introduce a function that counts the primes not exceeding a specified number.

Definition. The function $\pi(x)$, where x is a positive real number, denotes the number of primes not exceeding x.

ERATOSTHENES (c. 276–194 B.C.E.) was born in Cyrene, which was a Greek colony west of Egypt. It is known that he spent some time studying at Plato's school in Athens. King Ptolemy II invited Eratosthenes to Alexandria to tutor his son. Later, Eratosthenes became the chief librarian of the famous library at Alexandria, which was a central repository of ancient works of literature, art, and science. He was an extremely versatile scholar, having written on mathematics, geography, astronomy, history, philosophy, and literature. Besides his work in mathematics, Eratosthenes was most noted for his chronology of ancient history and for his geographical measurements, including his famous measurement of the size of the earth.

Example 3.3. From our illustration of the sieve of Eratosthenes, we see that $\pi(10) = 4$ and $\pi(100) = 25$. ◀

Primes in Arithmetic Progressions Every odd integer is either of the form $4n + 1$ or the form $4n + 3$. Are there infinitely many primes in both these forms? The primes 5, 13, 17, 29, 37, 41, ... are of the form $4n + 1$, and the primes 3, 7, 11, 19, 23, 31, 43, ... are of the form $4n + 3$. Looking at this evidence hints that there are infinitely many primes in both these progressions. What about other arithmetic progressions such as $3n + 1$, $7n + 4$, $8n + 7$, and so on? Does each of these contain infinitely many primes? German mathematician *G. Lejeune Dirichlet* settled this question in 1837, when he used methods from complex analysis to prove the following theorem.

Theorem 3.3. ***Dirichlet's Theorem on Primes in Arithmetic Progressions.*** Suppose that a and b are relatively prime positive integers. Then the arithmetic progression $an + b$, $n = 1, 2, 3, \ldots$, contains infinitely many primes.

No simple proof of Dirichlet's theorem on primes in arithmetic progressions is known. (Dirichlet's original proof used complex variables. In the 1950s, elementary but complicated proofs were found by Erdős and by Selberg.) However, special cases of Dirichlet's theorem can be proved quite easily. We will illustrate this in Section 3.5, by showing that there are infinitely many primes of the form $4n + 3$.

The Largest Known Primes For hundreds if not thousands of years, professional and amateur mathematicians have been motivated to find a prime larger than any currently known. The person who discovers such a prime becomes famous, at least for a time, and has his or her name entered into the record books. Because there are infinitely many prime numbers, there is always a prime larger than the current record. Looking for new primes is done somewhat systematically; rather than checking randomly, people examine numbers that have a special form. For example, in Chapter 7 we will discuss primes of the form $2^p - 1$, where p is prime; such numbers are called *Mersenne primes*. We will see that there is a special test that makes it possible to determine whether $2^p - 1$ is

G. LEJEUNE DIRICHLET (1805–1859) was born into a French family living in the vicinity of Cologne, Germany. He studied at the University of Paris when this was an important world center of mathematics. He held positions at the University of Breslau and the University of Berlin, and in 1855 was chosen to succeed Gauss at the University of Göttingen. Dirichlet is said to be the first person to master Gauss's *Disquisitiones Arithmeticae*, which had appeared 20 years earlier. He is said to have kept a copy of this book at bis side even when he traveled. His book on number theory, *Vorlesungen über Zahlentheorie*, helped make Gauss's discoveries accessible to other mathematicians. Besides bis fundamental work in number theory, Dirichlet made many important contributions to analysis. His famous "drawer principle," also called the pigeonhole principle, is used extensively in combinatorics and in number theory.

prime without performing trial divisions. The largest known prime number has been a Mersenne prime for most of the past hundred years. Currently, the world record for the largest prime known is $2^{43,112,609} - 1$.

Formulas for Primes Is there a formula that generates only primes? This is another question that has interested mathematicians for many years. No polynomial in one variable has this property, as Exercise 23 demonstrates. It is also the case that no polynomial in n variables, where n is a positive integer, generates only primes (a result that is beyond the scope of this book). There are several impractical formulas that generate only primes. For example, Mills has shown that there is a constant Θ such that the function $f(n) = [\Theta^{3^n}]$ generates only primes. Here the value of Θ is known only approximately, with $\Theta \approx 1.3064$. This formula is impractical for generating primes not only because the exact value of Θ is not known, but also because to compute Θ you must know the primes that $f(n)$ generates (see [Mi47] for details).

If no useful formula can be used to generate large primes, how can they be generated? In Chapter 6, we will learn how to generate large primes using what are known as probabilistic primality tests.

Primality Proofs

If someone presents you with a positive integer n and claims that n is prime, how can you be sure that n really is prime? We already know that we can determine whether n is prime by performing trial divisions of n by the primes not exceeding $\sqrt{n}$. If n is not divisible by any of these primes, it itself is prime. Consequently, once we have determined that n is not divisible by any prime not exceeding its square root, we have produced a proof that n is prime. Such a proof is also known as a *certificate of primality*.

Unfortunately, using trial division to produce a certificate of primality is extremely inefficient. To see this, we estimate the number of bit operations used by this test. Using the prime number theorem, we can estimate the number of bit operations needed to show that an integer n is prime by trial divisions of n by all primes not exceeding $\sqrt{n}$. The prime number theorem tells us that there are approximately $\sqrt{n}/\log \sqrt{n} = 2\sqrt{n}/\log n$ primes not exceeding $\sqrt{n}$. To divide n by an integer m takes $O(\log_2 n \cdot \log_2 m)$ bit operations. Therefore, the number of bit operations needed to show that n is prime by this method is at least $(2\sqrt{n}/\log n)(c \log_2 n) = c\sqrt{n}$ (where we have ignored the $\log_2 m$ term because it is at least 1, even though it sometimes is as large as $(\log_2 n)/2$). This method of showing that an integer n is prime is very inefficient, for it is necessary not only to know all the primes not larger than $\sqrt{n}$, but to do at least a constant multiple of $\sqrt{n}$ bit operations.

To input an integer into a computer program, we input the binary digits of the integer. Consequently, the computational complexity of algorithms for determining whether an integer is prime is measured in terms of the number of binary digits in the integer. By Exercise 11 in Section 2.3, we know that a positive integer n has $[\log_2 n] + 1$ binary digits. Consequently, a big-O estimate for the computational complexity of an algorithm in terms of number of binary digits of n translates to the same big-O estimate in terms of $\log_2 n$, and vice versa. Note that the algorithm using trial divisions to determine whether

an integer n is prime is exponential in terms of the number of binary digits of n, or in terms of $\log_2 n$, because $\sqrt{n} = 2^{\log_2 n/2}$. That is, this algorithm has exponential time complexity, measured in terms of the number of binary digits in n. As n gets large, an algorithm with exponential complexity quickly becomes impractical. Determining whether a number with 200 digits is prime using trial division still takes billions of years on the fastest computers.

Mathematicians have looked for efficient primality tests for many years. In particular, they have searched for an algorithm that produces a certificate of primality in polynomial time, measured in terms of the number of binary digits of the integer input. In 1975, G. L. Miller developed an algorithm that can prove that an integer is prime using $O((\log n)^5)$ bit operations, assuming the validity of a hypothesis called the generalized Riemann hypothesis. Unfortunately, the generalized Riemann hypothesis remains an open conjecture. In 1983, Leonard Adleman, Carl Pomerance, and Robert Rumely developed an algorithm that can prove an integer is prime using $(\log n)^{c \log\log\log n}$ bit operations, where c is a constant. Although their algorithm does not run in polynomial time, it runs in close to polynomial time because the function $\log\log\log n$ grows so slowly. To use their algorithm with an up-to-date PC to determine whether a 100-digit integer is prime requires just a few milliseconds, determining whether a 400-digit integer is prime requires less than a second, and determining whether a 1000-digit integer is prime takes less than an hour. (For more information about their test, see [AdPoRu83] and [Ru83].)

A Polynomial Time Algorithm for Prime Certificates Until 2002, no one was able to find a polynomial time algorithm for proving that a positive integer is prime. In 2002, M. Agrawal, N. Kayal, and N. Saxena, an Indian computer science professor and two of his undergraduate students, announced that they had found an algorithm that can produce a certificate of primality for an integer n using $O((\log n)^{12})$ bit operations. Their discovery of a polynomial time algorithm for proving that a positive integer is prime surprised the mathematical community. Their announcement stated that "*PRIMES* is in *P*." Here, computer scientists denote by *PRIMES* the problem of determining whether a given integer n is prime, and P denotes the class of problems that can be solved in polynomial time. Consequently, *PRIMES* is in P means that one can determine whether n is prime using an algorithm that has computational complexity bounded by a polynomial in the number of binary digits in n, or equivalently, in $\log n$. Their proof can be found in [AgKaSa02] and can be understood by undergraduate students who have studied number theory and abstract algebra. In this paper, they also show that under the assumption of a widely believed conjecture about the density of *Sophie Germain primes* (see Chapter 13 for a biography of the French mathematician Sophie Germain) [1] (primes p for which $2p + 1$ is also prime), their algorithm uses only $O((\log n)^6)$ bit operations. Other mathematicians have also improved on Agrawal, Kayal, and Saxena's result. In particular, H. Lenstra and C. Pomerance have reduced the exponent 12 in the original estimate to $6 + \epsilon$, where ϵ is any positive real number.

[1] Both the first name and last name of Sophie Germain are used to describe primes p for which $2p + 1$ is also prime. This type of terminology is rarely used when the names of other mathematicians are used as adjectives.

It is important to note that in our discussion of primality tests, we have only addressed *deterministic* algorithms, that is, algorithms that decide with certainty whether an integer is prime. In Chapter 6, we will introduce the notion of probabilistic primality tests, that is, tests that tell us that there is a high probability, but not a certainty, that an integer is prime.

3.1 Exercises

1. Determine which of the following integers are primes.

a) 101 c) 107 e) 113

b) 103 d) 111 f) 121

2. Determine which of the following integers are primes.

a) 201 c) 207 e) 213

b) 203 d) 211 f) 221

3. Use the sieve of Eratosthenes to find all primes less than 150.

4. Use the sieve of Eratosthenes to find all primes less than 200.

5. Find all primes that are the difference of the fourth powers of two integers.

6. Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.

7. Show that if a and n are positive integers with $n > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime. (*Hint:* Use the identity $a^{kl} - 1 = (a^k - 1)(a^{k(l-1)} + a^{k(l-2)} + \cdots + a^k + 1)$.)

8. (This exercise constructs another proof of the infinitude of primes.) Show that the integer $Q_n = n! + 1$, where n is a positive integer, has a prime divisor greater than n. Conclude that there are infinitely many primes.

9. Can you show that there are infinitely many primes by looking at the integers $S_n = n! - 1$, where n is a positive integer?

10. Using Euclid's proof that there are infinitely many primes, show that the nth prime p_n does not exceed $2^{2^{n-1}}$ whenever n is a positive integer. Conclude that when n is a positive integer, there are at least $n + 1$ primes less than 2^{2^n}.

11. Let $Q_n = p_1 p_2 \cdots p_n + 1$, where $p_1, p_2, \ldots, p_n$ are the n smallest primes. Determine the smallest prime factor of Q_n for $n = 1, 2, 3, 4, 5$, and 6. Do you think that Q_n is prime infinitely often? (*Note:* This is an unresolved question.)

12. Show that if p_k is the kth prime, where k is a positive integer, then $p_n \leq p_1 p_2 \cdots p_{n-1} + 1$ for all integers n with $n \geq 3$.

13. Show that if the smallest prime factor p of the positive integer n exceeds $\sqrt[3]{n}$, then n/p must be prime or 1.

14. Show that if p is a prime in the arithmetic progression $3n + 1$, $n = 1, 2, 3, \ldots$, then it is also in the arithmetic progression $6n + 1$, $n = 1, 2, 3, \ldots$.

15. Find the smallest prime in the arithmetic progression $an + b$, for these values of a and b:

a) $a = 3, b = 1$ b) $a = 5, b = 4$ c) $a = 11, b = 16$

16. Find the smallest prime in the arithmetic progression $an + b$, for these values of a and b:

a) $a = 5, b = 1$ b) $a = 7, b = 2$ c) $a = 23, b = 13$

17. Use Dirichlet's theorem to show that there are infinitely many primes whose decimal expansion ends with a 1.

18. Use Dirichlet's theorem to show that there are infinitely many primes whose decimal expansion ends with the two digits 23.

19. Use Dirichlet's theorem to show that there are infinitely many primes whose decimal expansion ends with the three digits 123.

20. Show that for every positive integer n there is a prime whose decimal expansion ends with at least n 1s.

* **21.** Show that for every positive integer n there is a prime whose decimal expansion contains n consecutive 1s and whose final digit is 3.

* **22.** Show that for every positive integer n there is a prime whose decimal expansion contains n consecutive 2s and whose final digit is 7.

23. Use the second principle of mathematical induction to prove that every integer greater than 1 is either prime or the product of two or more primes.

* **24.** Use the principle of inclusion–exclusion (Exercise 16 of Appendix B) to show that

$$\pi(n) = (\pi(\sqrt{n}) - 1) + n - \left(\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_r} \right\rfloor\right) + \left(\left\lfloor \frac{n}{p_1 p_2} \right\rfloor + \left\lfloor \frac{n}{p_1 p_3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_{r-1} p_r} \right\rfloor\right) - \left(\left\lfloor \frac{n}{p_1 p_2 p_3} \right\rfloor + \left\lfloor \frac{n}{p_1 p_2 p_4} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_{r-2} p_{r-1} p_r} \right\rfloor\right) + \cdots,$$

where $p_1, p_2, \ldots, p_r$ are the primes less than or equal to $\sqrt{n}$ (with $r = \pi(\sqrt{n})$). (*Hint:* Let property P_i be the property that an integer is divisible by p_i.)

25. Use Exercise 24 to find $\pi(250)$.

26. Show that $x^2 - x + 41$ is prime for all integers x with $0 \leq x \leq 40$. Show, however, that it is composite for $x = 41$.

27. Show that $2n^2 + 11$ is prime for all integers n with $0 \leq n \leq 10$, but is composite for $n = 11$.

28. Show that $2n^2 + 29$ is prime for all integers n with $0 \leq n \leq 28$, but is composite for $n = 29$.

* **29.** Show that if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $n \geq 1$ and the coefficients are integers, then there is a positive integer y such that $f(y)$ is composite. (*Hint:* Assume that $f(x) = p$ is prime, and show that p divides $f(x + kp)$ for all integers k. Conclude that there is an integer y such that $f(y)$ is composite from the fact that a polynomial of degree n, $n > 1$, takes on each value at most n times.)

The *lucky numbers* are generated by the following sieving process: Start with the positive integers. Begin the process by crossing out every second integer in the list, starting your count with the integer 1. Other than 1, the smallest integer not crossed out is 3, so we continue by crossing out every third integer left, starting the count with the integer 1. The next integer left is 7, so we cross out every seventh integer left. Continue this process, where at each stage we cross out every kth integer left, where k is the smallest integer not crossed out, other than 1, not yet used in the sieving process. The integers that remain are the lucky numbers.

30. Find all lucky numbers less than 100.

31. Show that there are infinitely many lucky numbers.

32. Suppose that t_k is the smallest prime greater than $Q_k = p_1 p_2 \cdots p_k + 1$, where p_j is the jth prime number.

a) Show that $t_k - Q_k + 1$ is not divisible by p_j for $j = 1, 2, \ldots, k$.

b) R. F. Fortune conjectured that $t_k - Q_k + 1$ is prime for all positive integers k. Show that this conjecture is true for all positive integers k with $k \leq 5$.

Computations and Explorations

1. Find the nth prime, where n is each of the following integers.

a) 1,000,000 b) 333,333,333 c) 1,000,000,000

2. Find the smallest prime greater than each of the following integers.

a) 1,000,000 b) 100,000,000 c) 100,000,000,000

3. Plot the nth prime as a function of n for $1 \leq n \leq 100$.

4. Plot $\pi(x)$ for $1 \leq x \leq 1000$.

5. Find the smallest prime factor of $n! + 1$ for all positive integers n not exceeding 20.

6. Find the smallest prime factor of $p_1 p_2 \cdots p_k + 1$, where $p_1, p_2, \ldots, p_k$ are the kth smallest primes for all positive integers k not exceeding 100. Which of these numbers are prime? For which of those that are not prime is p_{k+1} the smallest prime divisor of this number?

7. Find the smallest prime factor of $p_1 p_2 \cdots p_k - 1$, where $p_1, p_2, \ldots, p_k$ are the kth smallest primes for all positive integers k not exceeding 100. Which the numbers are primes? For which of those that are not prime is p_{k+1} the smallest prime divisor of this number?

8. The *Euler-Mullin sequence* $q_1, q_2, \ldots, q_k, \ldots$ is defined by taking $q_1 = 2$ and defining q_{k+1} to be the smallest prime factor of $q_1 q_2 \cdots q_k + 1$ whenever k is a positive integer. Find as many terms of this sequence as you can. It has been conjectured that this sequence is a reordering of the list of prime numbers.

9. Use the sieve of Eratosthenes to find all primes less than 10,000.

10. Use the result given in Exercise 18 to find $\pi(10{,}000)$, the number of primes not exceeding 10,000.

11. A famous unsettled conjecture of Hardy and Littlewood, now generally believed to be false, asserts that $\pi(x + y) \leq \pi(x) + \pi(y)$ for all integers x and y both greater than 1. Explore this conjecture by examining $\pi(x + y) - (\pi(x) + \pi(y))$ for various values of x and y.

12. Verify R. F. Fortune's conjecture that $t_k - Q_k + 1$ is prime for all positive integers k, where t_k is the smallest prime greater than $Q_k = \prod_{j=1}^{k} p_j + 1$ for as many k as you can.

13. Find all lucky numbers (as defined in the preamble to Exercise 30) not exceeding 10,000.

Programming Projects

1. Given a positive integer n, determine whether it is prime using trial division of the integer by all primes not exceeding its square root.

* **2.** Given a positive integer n, use the sieve of Eratosthenes to find all primes not exceeding it.

* **3.** Given a positive integer n, use Exercise 24 to find $\pi(n)$.

4. Given positive integers a and b not divisible by the same prime, find the smallest prime number in the arithmetic progression $an + b$, where n is a positive integer.

* **5.** Given a positive integer n, find the lucky numbers less than n (see the preamble to Exercise 30).

3.2 The Distribution of Primes

We know that there are infinitely many primes, but can we estimate how many primes there are less than a positive real number x? One of the most famous theorems of number theory, and of all mathematics, is the *prime number theorem,* which answers this question.

Mathematicians in the late eighteenth century examined tables of prime numbers created using hand calculations. Using these values, they looked for functions that estimated $\pi(x)$. In 1798, French mathematician Adrien-Marie Legendre (see Chapter 11 for a biography) used tables of primes up to 400,031, computed by Jurij Vega, to note that $\pi(x)$ could be approximated by the function

$$\frac{x}{\log x - 1.08366}.$$

The great German mathematician Karl Friedrich Gauss (see Chapter 4 for a biography) conjectured that $\pi(x)$ increases at the same rate as the functions

$$x/\log x \quad \text{and} \quad \text{Li}(x) = \int_2^x \frac{dt}{\log t}$$

(where $\int_2^x \frac{dt}{\log t}$ represents the area under the curve $y = 1/\log t$ and above the t-axis from $t = 2$ to $t = x$). (The name *Li* is an abbreviation of *logarithmic integral.*)

Neither Legendre nor Gauss managed to prove that these functions approximated $\pi(x)$ closely for large values of x. By 1811, a table of all primes up to 1,020,000 had been produced (by Chernac), which could be used to provide evidence for these conjectures.

The first substantial result showing that $\pi(x)$ could be approximated by $x/\log x$ was established in 1850 by Russian mathematician *Pafnuty Lvovich Chebyshev.* He showed that there are positive real numbers C_1 and C_2, with $C_1 < 1 < C_2$, such that

$$C_1(x/\log x) < \pi(x) < C_2(x/\log x)$$

for sufficiently large values of x. (In particular, he showed that this result holds with $C_1 = 0.929$ and $C_2 = 1.1$.) He also demonstrated that if the ratio of $\pi(x)$ and $x/\log x$ approaches a limit as x increases, then this limit must be 1.

The prime number theorem, which states that the ratio of $\pi(x)$ and $x/\log x$ approaches 1 as x grows without bound, was finally proved in 1896, when French mathematician *Jacques Hadamard* and Belgian mathematician *Charles-Jean-Gustave-Nicholas de la Vallée-Poussin* produced independent proofs. Their proofs were based

on results from the theory of complex analysis. They used ideas developed in 1859 by German mathematician Bernhard Riemann, which related $\pi(x)$ to the behavior of the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

in the complex plane. (The function $\zeta(s)$ is known as the *Riemann zeta function*.) The connection between the Riemann zeta function and the prime numbers comes from the identity

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} (1 - \frac{1}{p^s})^{-1},$$

where the product on the right-hand side of the equation extends over all primes p. We will explain why this identity is true in Section 3.5. (For information about the famous Riemann hypothesis, a conjecture about the roots of the zeta function, see the boxed note later in this section.)

PAFNUTY LVOVICH CHEBYSHEV (1821–1894) was born on the estate of his parents in Okatovo, Russia. His father was a retired army officer. In 1832, Chebyshev's family moved to Moscow, where he completed his secondary education with study at home. In 1837, Chebyshev entered Moscow University, graduating in 1841. While still an undergraduate, he made his first original contribution, a new method for approximating roots of equations. Chebyshev joined the faculty of St. Petersburg University in 1843, where he remained until 1882. His doctoral thesis, written in 1849, was long used as a number theory textbook at Russian universities. Chebyshev made contributions to many areas of mathematics besides number theory, including probability theory, numerical analysis, and real analysis. He worked in theoretical and applied mechanics, and had a bent for constructing mechanisms, including linkages and hinges. He was a popular teacher, and had a strong influence on the development of Russian mathematics.

JACQUES HADAMARD (1865–1963) was born in Versailles, France. His father was a Latin teacher and his mother a distinguished piano teacher. After completing his undergraduate studies, he taught at a Paris secondary school. After receiving his doctorate in 1892, he became lecturer at the Faculté des Sciences of Bordeaux. He subsequently served on the faculties of the Sorbonne, the Collège de France, the École Polytechnique, and the École Centrale des Arts et Manufactures. Hadamard made important contributions to complex analysis, functional analysis, and mathematical physics. His proof of the prime number theorem was based on his work in complex analysis. Hadamard was a famous teacher; he wrote numerous articles about elementary mathematics that were used in French schools, and his text on elementary geometry was used for many years.

In addition to proving the prime number theorem, de la Vallée-Poussin showed that the function $\mathrm{Li}(x)$ is a closer approximation to $\pi(x)$ than $x/(\log x - a)$ for all values of the constant a.

The proofs of the prime number theorem found by Hadamard and de la Valleé-Poussin depend on complex analysis, though the theorem itself does not involve complex numbers. This left open the challenge of finding a proof that did not use the theory of complex variables. It surprised the mathematical community when, in 1949, Norwegian mathematician *Atle Selberg* and Hungarian mathematician *Paul Erdős* independently found elementary proofs of the prime number theorem. Their proofs, though elementary (meaning that they do not use the theory of complex variables), are quite complicated and difficult.

We now formally state the prime number theorem.

Theorem 3.4. ***The Prime Number Theorem.*** The ratio of $\pi(x)$ to $x/\log x$ approaches 1 as x grows without bound. (Here, $\log x$ denotes the natural logarithm of x, and in the language of limits, we have $\lim_{x\to\infty} \pi(x)/(x/\log x) = 1$.)

CHARLES-JEAN-GUSTAVE-NICHOLAS DE LA VALLEÉ-POUSSIN (1866–1962), the son of a geology professor, was born at Louvain, Belgium. He studied at the Jesuit College at Mons, first studying philosophy, later turning to engineering. After receiving his degree, instead of pursuing a career in engineering, he devoted himself to mathematics. De la Valleé-Poussin's most significant contribution to mathematics was his proof of the prime number theorem. Extending this work, he established results about the distribution of primes in arithmetic progressions and the distribution of primes represented by quadratic forms. Furthermore, he refined the prime number theorem to include error estimates. He made important contributions to differential equations, approximation theory, and analysis. His textbook, *Cours d'analyse*, had a strong impact on mathematical thought in the first half of the twentieth century.

ATLE SELBERG (1917–2007), born in Langesund, Norway, became interested in mathematics as a schoolboy. He was inspired by Ramanujan's writing, both by the mathematics and the "air of mystery" surrounding Ramanujan's personality. Selberg received his doctorate in 1943 from the University of Oslo. He remained at the university until 1947, when he married and took a position at the Institute for Advanced Study in Princeton. After a brief stay at Syracuse University, he returned to the Institute for Advanced Study, where he was appointed a permanent member in 1949; he became a professor at Princeton University in 1951. Selberg received the Fields Medal, the most prestigious award in mathematics, for bis work on sieve methods and on the properties of the set of zeros of the Riemann zeta function. He is also well known for bis elementary proofs of the prime number theorem (also done by Paul Erdős), Dirichlet's theorem on primes in arithmetic progressions, and the generalization of the prime number theorem for primes in arithmetic progressions.

Remark. A concise way to state the prime number theorem is to write $\pi(x) \sim x/\log x$. Here, the symbol $\sim$ denotes "is asymptotic to." We write $a(x) \sim b(x)$ to denote that $\lim_{x\to\infty} a(x)/b(x) = 1$, and we say that $a(x)$ is asymptotic to $b(x)$.

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$	$Li(x)$	$\pi(x)/Li(x)$
10^3	168	144.8	1.160	178	0.9438202
10^4	1229	1085.7	1.132	1246	0.9863563
10^5	9592	8685.9	1.104	9630	0.9960540
10^6	78498	72382.4	1.085	78628	0.9983466
10^7	664579	620420.7	1.071	664918	0.9998944
10^8	5761455	5428681.0	1.061	5762209	0.9998691
10^9	50847534	48254942.4	1.054	50849235	0.9999665
10^{10}	455052512	434294481.9	1.048	455055614	0.9999932
10^{11}	4118054813	3948131663.7	1.043	4118165401	0.9999731
10^{12}	37607912018	36191206825.3	1.039	37607950281	0.9999990
10^{13}	346065536839	334072678387.1	1.036	346065645810	0.9999997
10^{14}	3204941750802	3102103442166.0	1.033	3204942065692	0.9999999

Table 3.1 *Approximations to* $\pi(x)$.

PAUL ERDŐS (1913–1996), born in Budapest, Hungary, was the son of high school mathematics teachers. When he was three years old, he could multiply three-digit numbers in his head, and when he was four, he discovered negative numbers on his own. At 17, he entered Eötvős University, graduating in four years with a Ph.D. in mathematics. After graduating, he spent four years at Manchester University, England, as a postdoctoral fellow. In 1938, he came to the United States because of the difficult political situation in Hungary, especially for Jews.

Erdős made many significant contributions to combinatorics and to number theory. One of the discoveries of which he was most proud was his elementary proof of the prime number theorem. He also participated in the modern development of Ramsey theory, a part of combinatorics. Erdős traveled extensively throughout the world to work with other mathematicians. He traveled from one mathematician or group of mathematicians to the next, proclaiming, "My brain is open." Erdős offered monetary rewards for the solutions of problems he found particularly interesting. Erdős wrote more than 1500 papers, with almost 500 coauthors. These coauthors are said to have *Erdős number* one. Otherwise, a mathematician's Erdős number is $k+1$ if the smallest Erdős number of his or her coauthors is k. Two fascinating biographies ([Sc98] and [Ho99]) and the film *N is a Number* [Cs07] give further details on his life and work.

The prime number theorem tells us that the ratio between $x/\log x$ and $\pi(x)$ is close to 1 when x is large. However, there are functions for which the ratio between these functions and $\pi(x)$ approaches 1 more rapidly than it does for $x/\log x$. In particular, it has been shown that $\mathrm{Li}(x)$ is an even better approximation. In Table 3.1, we see evidence for the prime number theorem and that $\mathrm{Li}(x)$ is an excellent approximation of $\pi(x)$. (Note that the values of $\mathrm{Li}(x)$ have been rounded to the nearest integer.)

The Riemann Hypothesis

Many mathematicians consider the *Riemann hypothesis*, a conjecture about the zeros of the zeta function, the most important open problem in pure mathematics. For more than 100 years, number theorists have struggled to solve this problem. Interest in it has spread, perhaps because a prize of one million dollars for a proof (if it is indeed true) has been offered by the Clay Mathematics Institute. Recently, many general-interest books about the Riemann hypothesis, such as [De03], [Sa03a], and [Sa03b], have appeared, even though the hypothesis involves sophisticated notions from complex analysis. We will briefly describe the Riemann hypothesis for the benefit of readers familiar with complex analysis, as well as for the general appreciation of others.

We have defined the Riemann zeta function as $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. This definition is valid for all complex numbers s with $Re(s) > 1$, where $Re(s)$ is the real part of the complex number s. Riemann was able to extend the function defined by the infinite series to a function in the entire complex plane with a pole at $s = 1$. In his famous 1859 paper [Ri59], Riemann connected the zeta function with the distribution of prime numbers. He derived a formula for $\pi(x)$ in terms of the zeros of $\zeta(s)$. The more we understand about the location of the zeros of the zeta function, the more we know about the distribution of the primes. The Riemann hypothesis is a statement about the location of the zeros of this function. Before stating the hypothesis, we first note that the zeta function has zeros at the negative even integers $-2, -4, -6, \ldots$, called the *trivial zeros*. The Riemann hypothesis is the assertion that the nontrivial zeros of $\zeta(s)$ all have real part equal to 1/2. Note that there is an equivalent formulation of the Riemann hypothesis in terms of the error introduced when $\mathrm{Li}(x)$ is used to estimate $\pi(x)$; this alternative formulation does not involve complex variables. In 1901, von Koch showed that the Riemann hypothesis is equivalent to the statement that the error that occurs when $\pi(x)$ is estimated by $\mathrm{Li}(x)$ is $O(x^{1/2} \log x)$.

Many mathematicians believe the Riemann hypothesis is true, particularly because of the wealth of evidence supporting it. First, a vast amount of numerical evidence has been found. We now know that the first 2.5×10^{11} zeros (in order of increasing imaginary parts) have real part equal to 1/2. (These computations were done by Sebastian Wedeniwski, who has set up a distributed computing project to carry them out called ZetaGrid). Second, we know that at least 40% of the nontrivial zeros of the zeta function are simple and have real part equal to 1/2. Third, we know that if there are exceptions to the Riemann hypothesis, they must be rare as we move away from the line $Re(s) = 1/2$. Of course, it is still possible that this evidence is misleading us and that the Riemann hypothesis is not true. Perhaps this famous problem will be resolved in the next few years, or maybe it will resist all attacks for hundreds of years into the future. For more information about the Riemann hypothesis, consult [Ed01] and the online essay by Enrico Bombieri on the Web site for the Clay Institute Millenium Prize Problems.

It is not necessary to find all primes not exceeding x to compute $\pi(x)$. One way to evaluate $\pi(x)$ without finding all the primes less than x is to use a counting argument based on the sieve of Eratosthenes (see Exercise 18 in Section 3.1). Efficient ways of computing $\pi(x)$ requiring only $O(x^{(3/5)+\epsilon})$ bit operations have been devised by Lagarias and Odlyzko [LaOd82]. The world record is currently held by Tomás Oliveira e Silva, who was able to compute $\pi(10^{23}) = 1{,}925{,}320{,}391{,}606{,}803{,}968{,}923$ in 2008.

How big is the nth prime? From the prime number theorem, we know that that $n = \pi(p_n) \sim p_n/\log p_n$. Because taking logarithms of both sides of an asymptotic formula maintains the asymptotic relationship, we find that $\log n \sim \log(p_n/\log p_n) = \log p_n - \log\log p_n \sim \log p_n$. Consequently, $p_n \sim n \log p_n \sim n \log n$. We state this fact as a corollary.

Corollary 3.4.1. Let p_n be the nth prime, where n is a positive integer. Then $p_n \sim n \log n$. That is, the nth prime is asymptotic to $\log n$.

What is the probability that a randomly selected positive integer is prime? Given that there are approximately $x/\log x$ primes not exceeding x, the probability that x is prime is approximately $(x/\log x)/x = 1/\log x$. For example, the probability that an integer near 10^{1000} is prime is approximately $1/\log 10^{1000} \approx 1/2302$. Suppose that you want to find a prime with 1000 digits; what is the expected number of integers you must select before you find a prime? The answer is that you must select roughly $1/(1/2302) = 2302$ integers of this size before one of them will be a prime. Of course, you will need to check each one to determine whether it is prime. In Chapter 6, we will discuss how this can be done efficiently.

Gaps in the Distribution of Primes We have shown that there are infinitely many primes and we have discussed the abundance of primes below a given bound x, but we have yet to discuss how regularly primes are distributed throughout the positive integers. We first give a result that shows that there are arbitrarily long runs of integers containing no primes.

One of the Largest Numbers Ever Appearing Naturally in a Proof

Using the data in Table 3.1, we can show that for all x in the table, the difference $\mathrm{Li}(x) - \pi(x)$ is positive and increases as x grows. Gauss, who only had access to the data in the first few rows of this table, believed this trend held for all positive integers x. However, in 1914, the English mathematician J. E. Littlewood showed that $\mathrm{Li}(x) - \pi(x)$ changes sign infinitely many times. In his proof, Littlewood did not establish a lower bound for the first time that $\mathrm{Li}(x) - \pi(x)$ changes from positive to negative. This was done in 1933 by Samuel Skewes, a student of Littlewood's, who managed to show that $\mathrm{Li}(x) - \pi(x)$ changes signs for at least one x with $x < 10^{10^{10^{34}}}$, a humongous number. This number, known as *Skewes' constant*, became famous as the largest number to appear naturally in a mathematical proof. Fortunately, in the past seven decades, considerable progress has been made in reducing this bound. The best current results show that $\mathrm{Li}(x) - \pi(x)$ changes sign near $x = 1.39822 \times 10^{316}$.

Theorem 3.5. For any positive integer n, there are at least n consecutive composite positive integers.

Proof. Consider the n consecutive positive integers

$$(n+1)!+2, \quad (n+1)!+3, \quad \ldots, \quad (n+1)!+n+1.$$

When $2 \leq j \leq n+1$, we know that $j \mid (n+1)!$. By Theorem 1.9 it follows that $j \mid (n+1)!+j$. Hence, these n consecutive integers are all composite. ■

Example 3.4. The seven consecutive integers beginning with $8!+2 = 40{,}322$ are all composite. (However, these are much larger than the smallest seven consecutive composites, 90, 91, 92, 93, 94, 95, and 96.) ◀

Conjectures About Primes

Professional and amateur mathematicians alike find the prime numbers fascinating. It is not surprising that a tremendous variety of conjectures have been formulated concerning prime numbers. Some of these conjectures have been settled, but many still elude resolution. We will describe some of the best known of these conjectures here.

Looking at tables of primes led mathematicians in the first half of the nineteenth century to make conjectures that the distribution of primes satisfies some basic properties, such as this following conjecture.

Bertrand's Conjecture. In 1845, the French mathematician Joseph Bertrand conjectured that for every positive integer n with $n > 1$, there is a prime p such that $n < p < 2n$. Bertrand verified this conjecture for all n not exceeding 3,000,000, but he could not produce a proof. The first proof of this conjecture was found by Pafnuty Lvovich Chebyshev in 1852. Because this conjecture has been proved, it is often called *Bertrand's postulate*. (See Exercises 22–24 for an outline of a proof.)

Theorem 3.5 shows that the gap between consecutive primes is arbitrarily long. On the other hand, primes may often be close together. The only consecutive primes are 2

JOSEPH LOUIS FRANÇOIS BERTRAND (1822–1900) was born in Paris. He studied at the École Polytechnique from 1839 until 1841 and at the École des Mines from 1841 to 1844. Instead of becoming a mining engineer, he decided to become a mathematician. Bertrand was appointed to a position at the École Polytechnique in 1856, and, in 1862, he also became professor at the Collège de France. In 1845, on the basis of extensive numerical evidence in tables of primes, Bertrand conjectured that there is at least one prime between n and $2n$ for every integer n with $n > 1$. This result was first proved by Chebyshev in 1852. Besides working in number theory, Bertrand worked on probability theory and differential geometry. He wrote several brief volumes on the theory of probability and on analyzing data from observations. His book *Calcul des probabilitiés*, written in 1888, contains a paradox on continuous probabilities now known as Bertrand's paradox. Bertrand was considered to be kind at heart, extremely clever, and full of spirit.

and 3, because 2 is the only even prime. However, many pairs of primes differ by two; these pairs of primes are called *twin primes*. Examples are the pairs 3, 5 and 7, 11 and 13, 101 and 103, and 4967 and 4969.

Evidence seems to indicate that there are infinitely many pairs of twin primes. There are 35 pairs of twin primes less than 10^3; 8169 pairs less than 10^6; 3,424,506 pairs less than 10^9; and 1,870,585,220 pairs less than 10^{12}. This leads to the following conjecture.

Twin Prime Conjecture. There are infinitely many pairs of primes p and $p + 2$.

In 1966, Chinese mathematician J. R. Chen showed, using sophisticated sieve methods, that there are infinitely many primes p such that $p + 2$ has at most two prime factors. An active competition is under way to produce new largest pairs of twin primes. The current record for the largest pair of twin primes is $2{,}003{,}663{,}613 \cdot 2^{195{,}000} \pm 1$, a pair of primes with 58,711 digits each discovered in 2007.

The twin prime conjecture asserts that infinitely many primes occur as pairs of consecutive odd numbers. However, consecutive primes may be far apart. A consequence of the prime number theorem is that as n grows, the average gap between the consecutive primes p_n and p_{n+1} is $\log p_n$. Number theorists have worked hard to prove results that show that the gaps between consecutive primes are much smaller than average for infinitely many primes. In 2005, a breakthrough was made by Daniel Goldston, János Pintz, and Cem Yildrim. They showed that for every positive number c, there are infinitely many pairs of consecutive primes p_n and p_{n+1} that differ less than c times $\log p_n$, the average distance between consecutive primes. They also showed that under the assumption of a conjecture known as the Elliott-Halberstam conjectures, there are infinitely pairs of primes within 16 of each other.

Viggo Brun showed that the sum $\sum_{\text{primes } p \text{ with } p+2 \text{ prime}} \frac{1}{p} = (1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/13) + \cdots$ converges to a constant called *Brun's constant*, which is approximately equal to 1.9021605824. Surprisingly, the computation of Brun's constant has played a role in discovering flaws in Intel's original Pentium chip. In 1994, Thomas Nicely at Lynchburg College in Virginia computed Brun's constant in two different ways using different methods on a Pentium PC and came up with different answers. He traced the error back to a flaw in the Pentium chip and he alerted Intel to this problem. (See the box on page 89 for more information about Nicely's discovery.)

JING RUN CHEN (1933–1996) was a student of the prominent Chinese number theorist Loo Keng Hua. Chen was almost entirely devoted to mathematical research. During the Cultural Revolution in China, he continued his research, working almost all day and night in a tiny room with no electric lights, no table or chairs, only a small bed, and his books and papers. It was during this period that he made his most important discoveries concerning twin primes and Goldbach's conjecture. Although he was a mathematical prodigy, Chen was considered to be next to hopeless in other aspects of life. He died in 1996 after a long illness.

The Erdős Conjecture on Arithmetic Progressions of Primes. For every positive integer $n \geq 3$, there is an arithmetic progression of primes of length n.

This conjecture most likely dates back more than a century; it was discussed by Paul Erdős in the 1930s. Although much numerical evidence was found to support this conjecture, it remained unsettled for many years.

Example 3.5. The sequence 5, 11, 17, 23, 29 is an arithmetic progression of five primes and the sequence 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 is an arithmetic progression of ten primes, as the reader should verify. ◀

The Dutch mathematician Johannes van der Corput (1890–1971) made some progress on this conjecture when he showed in 1939 that there are infinitely many arithmetic progressions of three primes. In a major breakthrough, Ben Green and *Terrence Tao* were able to prove this conjecture in 2006. They began by attempting to show that there are infinitely many arithmetic progressions of four primes, but were able to prove the full conjecture, which is now known as the Green-Tao Theorem. Their proof, considered to be a mathematical tour de force, is a nonconstructive existence proof that combines ideas from several different areas of mathematics, including analytic number theory and ergodic theory. Because it is nonconstructive, it cannot be used to construct

TERRENCE TAO (born 1975) was born in Australia; His parents immigrated there from Hong Kong. His father is a pediatrician and his mother taught mathematics at a Hong Kong secondary school. Tao was a child prodigy. He taught himself arithmetic at the age of two. At 10, he became the youngest contestant at the International Mathematics Olympiad (IMO), later winning an IMO gold medal when he was 13. At 17, Tao received his bachelors and masters degrees and began graduate studies at Princeton University, receiving his Ph.D. in three years. In 1996, he became a faculty member at the University of California, Los Angeles, where he continues to work.

Tao is an extremely versatile mathematician who 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, which discusses progress on various problems. His most famous result is the Green-Tao Theorem, which tells that there are arbitrarily long arithmetic progressions of primes. Besides working in pure mathematics, Tao has made important contributions to the applications of mathematics. For example, he has made key contributions to the area of compressive sampling, which involves the reconstruction of digital images using the least possible 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, "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.

examples of arithmetic progressions of specified length. The Green-Tao theorem establishes a special case of a more general conjecture that Paul Erdős made in the 1930s, namely, that if the sum of the reciprocals of the elements of a set A of positive integers diverges, then A contains arbitrarily long arithmetic progressions. This more general conjecture remains unsettled.

We now discuss perhaps the most notorious conjecture about primes.

Goldbach's Conjecture. Every even positive integer greater than 2 can be written as the sum of two primes.

Example 3.6. The integers 10, 24, and 100 can be written as the sum of two primes in the following ways:

$$\begin{aligned} 10 &= 3+7 = 5+5, \\ 24 &= 5+19 = 7+17 = 11+13, \\ 100 &= 3+97 = 11+89 = 17+83 \\ &\quad = 29+71 = 41+59 = 47+53. \end{aligned}$$

◀

This conjecture was stated by *Christian Goldbach* in a letter to Leonhard Euler in 1742. It has been verified by a distributed computing effort for all even integers less than 10^{18}, with this limit increasing as computers become more powerful. Usually, there are many ways to write a particular even integer as the sum of primes, as Example 3.5 illustrates. However, a proof that there is always at least one way has not yet been found. The best result known to date is due to *J. R. Chen*, who showed (in 1966), using powerful sieve methods, that all sufficiently large integers are the sum of a prime and the product of at most two primes.

There are many conjectures concerning the number of primes of various forms, such as the following conjecture.

The $n^2 + 1$ Conjecture. There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer.

The smallest primes of the form $n^2 + 1$ are $2 = 1^2 + 1^2$, $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$, $101 = 10^2 + 1$, $197 = 14^2 + 1$, $257 = 16^2 + 1$, and $401 = 20^2 + 1$. The best

CHRISTIAN GOLDBACH (1690–1764) was born in Königsberg, Prussia (the city noted in mathematical circles for its famous bridge problem). He became professor of mathematics at the Imperial Academy of St. Petersburg in 1725. In 1728, Goldbach went to Moscow to tutor Tsarevich Peter II. In 1742, he entered the Russian Ministry of Foreign Affairs as a staff member. Goldbach is most noted for his correspondence with eminent mathematicians, in particular Leonhard Euler and Daniel Bernoulli. Besides his well-known conjectures that every even positive integer greater than 2 is the sum of two primes and that every odd positive integer greater than 5 is the sum of three primes, Goldbach made several notable contributions to analysis.

result known to date is that there are infinitely many integers n for which $n^2 + 1$ is either a prime or the product of two primes. This was shown by Henryk Iwaniec in 1973. Conjectures such as the $n^2 + 1$ conjecture may be easy to state, but are sometimes extremely difficult to resolve (see [Ri96] for more information).

We have discussed three of the four problems about primes described as "unattackable by the present state of science" in 1912 by the famous number theorist Edmund Landau in his address at the International Congress of Mathematicians. These four problems, known collectively as *Landau's problems*, are Goldbach's conjecture, the twin prime conjecture, the existence of infinitely many primes of the form $n^2 + 1$, and this conjecture of Legendre:

The Legendre Conjecture. There is a prime between every two pairs of consecutive squares of integers.

Pentium Chip Flaw

The story behind the Pentium chip flaw encountered by Thomas Nicely shows that answers produced by computers should not always be trusted. A surprising number of hardware and software problems arise that lead to incorrect computational results. This story also shows that companies risk serious problems when they hide errors in their products. In June 1994, testers at Intel discovered that Pentium chips did not always carry out computations correctly. However, Intel decided not to make public information about this problem. Instead, they concluded that because the error would not affect many users, it was unnecessary to alert the millions of owners of Pentium computers. The Pentium flaw involved an incorrect implementation of an algorithm for floating-point division. Although the probability is low that divisions of numbers affected by this error come up in a computation, such divisions arise in many computations in mathematics, science, and engineering, and even in spreadsheets running business applications.

Later in that same month, Nicely came up with two different results when he used a Pentium computer to compute Brun's constant in different ways. In October 1994, after checking all possible sources of computational error, Nicely contacted Intel customer support. They duplicated his computations and verified the existence of an error. Furthermore, they told him that this error had not been previously reported. After not hearing any additional information from Intel, Nicely sent e-mail to a few people telling them about this. These people forwarded the message to other interested parties, and within a few days, information about the bug was posted on an Internet newsgroup. By late November, this story was reported by CNN, the *New York Times*, and the Associated Press.

Surprised by the bad publicity, Intel offered to replace Pentium chips, but only for users running applications determined by Intel to be vulnerable to the Pentium division flaw. This offer did not mollify the Pentium user community. All the bad publicity drove Intel stock down several dollars a share and Intel became the object of many jokes, such as: "At Intel, quality is job 0.999999998." Finally, in December 1994, Intel decided to offer a replacement Pentium chip upon request. They set aside almost half a billion dollars to cover costs, and they hired hundreds of extra employees to handle customer requests. Nevertheless, this story does have a happy ending for Intel. Their corrected and improved version of the Pentium chip was extremely successful.

This conjecture was proposed by the French mathematician Adrien-Marie Legendre (see Chapter 11 for his biography). Numerical evidence for this conjecture shows that there is a prime between n^2 and $(n+1)^2$ for all $n \leq 10^{18}$. Note that Ingham has shown that for sufficiently large n, there is a prime between n^3 and $(n+1)^3$.

Although all four unsettled conjectures described by Landau in 1912 remain open, partial progress has been made on each. We may see one or more of them settled in the next few years. However, it may still be the case that all remain unsettled a century from now.

3.2 Exercises

1. Find the smallest five consecutive composite integers.

2. Find one million consecutive composite integers.

3. Show that there are no "prime triplets," that is, primes p, $p+2$, and $p+4$, other than 3, 5 , and 7.

4. Find the smallest four sets of prime triplets of the form p, $p+2$, $p+6$.

5. Find the smallest four sets of prime triplets of the form p, $p+4$, $p+6$.

6. Find the smallest prime between n and $2n$ for these values of n.

a) 3 b) 5 c) 19 d) 31

7. Find the smallest prime between n and $2n$ for these values of n.

a) 4 b) 6 c) 23 d) 47

8. Find the smallest prime between n^2 and $(n+1)^2$ for all positive integers n with $n \leq 10$.

9. Find the smallest prime between n^2 and $(n+1)^2$ for all positive integers n with $11 \leq n \leq 20$.

* **10.** Show that there are infinitely many primes that are not one of the primes in a pair of twin primes. (*Hint:* Apply Dirichlet's theorem.)

* **11.** Show that there are infinitely many primes that are not part of a prime triple of the form p, $p+2$, $p+6$. (*Hint:* Apply Dirichlet's theorem.)

12. Verify Goldbach's conjecture for each of the following values of n.

a) 50 c) 102 e) 200
b) 98 d) 144 f) 222

13. Goldbach also conjectured that every odd positive integer greater than 5 is the sum of three primes. Verify this conjecture for each of the following odd integers.

a) 7 c) 27 e) 101
b) 17 d) 97 f) 199

14. Show that every integer greater than 11 is the sum of two composite integers.

15. Show that Goldbach's conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the conjecture that every integer greater than 5 is the sum of three primes.

16. Let $G(n)$ denote the number of ways to write the even integer n as the sum $p+q$, where p and q are primes with $p \leq q$. Goldbach's conjecture asserts that $G(n) \geq 1$ for all even integers

n with $n > 2$. A stronger conjecture asserts that $G(n)$ tends to infinity as the even integer n grows without bound.

a) Find $G(n)$ for all even integers n with $4 \leq n \leq 30$.

b) Find $G(158)$. c) Find $G(188)$.

* **17.** Show that if n and k are positive integers with $n > 1$ and all n positive integers $a, a + k, \ldots, a + (n-1)k$ are odd primes, then k is divisible by every prime less than n.

Use Exercise 17 to help you solve Exercises 18–21.

18. Find an arithmetic progression of length six that begins with the integer 7 and where every term is a prime.

19. Find the smallest possible minimum difference for an arithmetic progression that contains four terms and where every term is a prime.

20. Find the smallest possible minimum difference for an arithmetic progression that contains five terms and where every term is a prime.

* **21.** Find the smallest possible minimum difference for an arithmetic progression that contains six terms and where every term is a prime.

22. a) In 1848, A. de Polignac conjectured that every odd positive integer is the sum of a prime and a power of two. Show that this conjecture is false by showing that 509 is a counterexample.

b) Find the next smallest counterexample after 509.

* **23.** A *prime power* is an integer of the form p^n, where p is prime and n is a positive integer greater than 1. Find all pairs of prime powers that differ by 1. Prove that your answer is correct.

* **24.** Let n be a positive integer greater than 1 and let $p_1, p_2, \ldots, p_t$ be the primes not exceeding n. Show that $p_1 p_2 \cdots p_t < 4^n$.

* **25.** Let n be a positive integer greater than 3 and let p be a prime such that $2n/3 < p \leq n$. Show that p does not divide the binomial coefficient $\binom{2n}{n}$.

** **26.** Use Exercises 24 and 25 to show that if n is a positive integer, then there exists a prime p such that $n < p < 2n$. (This is *Bertrand's conjecture.*)

27. Use Exercise 26 to show that if p_n is the nth prime, then $p_n \leq 2^n$.

28. Use Bertrand's conjecture to show that every positive integer n with $n \geq 7$ is the sum of distinct primes.

29. Use Bertrand's postulate to show that $\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+m}$ does not equal an integer when n and m are positive integers.

* **30.** In this exercise, we show that if n is an integer with $n \geq 4$, then $p_{n+1} < p_1 p_2 \cdots p_n$, where p_k is the kth prime. This result is known as *Bonse's inequality.*

a) Let k be a positive integer. Show that none of the integers $p_1 p_2 \cdots p_{k-1} \cdot 1 - 1$, $p_1 p_2 \cdots p_{k-1} \cdot 2 - 1, \ldots, p_1 p_2 \cdots p_{k-1} \cdot p_k - 1$ is divisible by one of the first $k-1$ primes and that if a prime p divides one of these integers, then it cannot divide another of these integers.

b) Conclude from part (a) that if $n - k + 1 < p_k$, then there is an integer among those listed in part (a) not divisible by p_j for $j = 1, \ldots, n$. (*Hint:* Use the pigeonhole principle.)

c) Use part (b) to show that if $n - k + 1 < p_k$, then $p_{n+1} < p_1 p_2 \cdots p_k$. Fix n and suppose that k is the least positive integer such that $n - k + 1 < p_k$. Show that $n - k \geq p_{k-1} - 2$

and that $p_{k-1} - 2 \geq k$ when $k \geq 5$ and that if $n \geq 10$, then $k \geq 5$. Conclude that if $n \geq 20$, then $p_{(n+1)} < p_2 p_2 \cdots p_k$ for some k with $n - k \geq k$. Use this to derive Bonse's inequality when $n \geq 10$.

d) Check the cases when $4 \leq n < 10$ to finish the proof.

31. Show that 30 is the largest integer n with the property that if $k < n$ and there is no prime p that divides both k and n, then k is prime. (*Hint:* Show that if n has this property and $n \geq p^2$ where p is prime, then $p \mid n$. Conclude that if $n \geq 7^2$, then n must be divisible by 2, 3, 5, and 7. Apply Bonse's inequality to show that such an n must be divisible by every prime, a contradiction. Show that 30 has the desired property, but no n with $30 < n < 49$ does.)

* **32.** Show that $p_{n+1}p_{n+2} < p_1 \cdot p_2 \cdots p_n$, where p_k is the kth prime whenever n is an integer with $n \geq 4$. (*Hint:* Use Bertrand's postulate and the work done in part (c) of the proof of Bonse's inequality.)

33. Show that $p_n^2 < p_{n-1}p_{n-2}p_{n-3}$, where p_k is the kth prime number and $n \geq 6$. Also, show that inequality does not hold when $n = 3$, 4, or 5. (*Hint:* Use Bertrand's postulate to obtain $p_n < 2p_{n-1}$ and $p_{n-1} < 2p_{n-2}$.)

34. Show that for every positive integer N there is an even number K so that there are more than N pairs of successive primes such that K is the difference between these successive primes. (*Hint:* Use the prime number theorem.)

35. Use Corollary 3.4.1 to estimate the millionth prime.

Computations and Explorations

1. Verify as much of the information given in Table 3.1 as you can.

2. Find as many terms as you can of the sequence of prime gaps d_n, $n = 1, 2, \ldots$.

3. Find as many tuples of primes of the form p, $p + 2$, and $p + 6$ as you can.

4. Verify Goldbach's conjecture for all even positive integers less than 10,000.

5. Find all twin primes less than 10,000.

6. Find the first pair of twin primes greater than each of the integers in Computation 1.

7. Plot $\pi_2(x)$, the number of twin primes not exceeding x, for $1 \leq x \leq 1000$ and $1 \leq x \leq 10{,}000$.

8. Hardy and Littlewood conjectured that $\pi_2(x)$, the number of twin primes not exceeding x, is asymptotic to $2C_2x/(\log x)^2$ where $C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)$. The constant C_2 is approximately equal to 0.66016. Determine how accurate this asymptotic formula for $\pi_2(x)$ is for values of x as large as you can compute.

9. Compute Brun's constant with as much accuracy as possible.

10. Explore the conjecture that $G(n)$, the number of ways the even integer n is the sum $p + q$, of primes $p \leq q$, satisfies $G(n) \geq 10$ for all even integers $n \geq 188$.

11. An unsettled conjecture asserts that for every positive integer n, there is an arithmetic progression of length n consisting of n consecutive prime numbers. The longest such arithmetic progression currently known consists of 22 consecutive primes. Find arithmetic progressions consisting of three consecutive primes with all primes less than 100 and four consecutive primes with all primes less than 500.

12. Show that all terms of the arithmetic progression of length five that begins with 1,464,481 and has common difference 210 are prime.

13. Show that all terms of the arithmetic progression of length twelve that begins with 23,143 and has common difference 30,030 are prime.
14. Find an arithmetic progression containing ten primes that begins with 199.
15. Andrica's conjecture, named after Dorin Adrica, claims that $A_n = \sqrt{p_{n+1}} - \sqrt{p_n} < 1$ for all positive integers n, where p_n denotes the nth prime. Gather evidence for this conjecture by computing A_n for as many positive integers n as you can. From your work, make a conjecture about the largest value of A_n.
16. Verify Legendre's conjecture for $n = 1000$, $n = 10{,}000$, $n = 100{,}000$, and $n = 1{,}000{,}000$.
17. Explore the conjecture that every even integer is the sum of two, not necessarily distinct, lucky numbers. Continue by exploring the conjecture that given a positive integer k, there is a positive integer n that can be expressed as the sum of two lucky numbers in exactly k ways.

Programming Projects

1. Given a positive integer n, verify Goldbach's conjecture for all even integers less than n.
2. Given a positive integer n, find all twin primes less than n.
3. Given a positive integer m, find the first m primes of the form $n^2 + 1$, where n is a positive integer.
4. Given an even positive integer n, find $G(n)$, the number of ways to write n as the sum $p + q$, where p and q are primes with $p \leq q$.
5. Given a positive integer n, find as many arithmetic progressions of length n, where every term is a prime.

3.3 Greatest Common Divisors and their Properties

We introduced the concept of the greatest common divisor of two integers in Section 1.5. Recall that the greatest common divisor of two integers a and b not both 0, denoted by (a, b), is the largest integer that divides both a and b. We also specified that $(0, 0) = 0$ to ensure that results we prove about greatest common divisors hold in all cases. In Section 1.5, we stated that two integers are called relatively prime if they share no common divisor greater than 1.

Note that since the divisors of $-a$ are the same as the divisors of a, it follows that $(a, b) = (|a|, |b|)$ (where $|a|$ denotes the absolute value of a, which equals a if $a \geq 0$ and $-a$ if $a < 0$). Hence, we can restrict our attention to the greatest common divisors of pairs of positive integers.

In Example 1.37, we noted that $(15, 81) = 3$. If we divide 15 and 81 by $(15, 81) = 3$, we obtain two relatively prime integers, 5 and 27. This is no surprise, because we have removed all common factors. This illustrates the following theorem, which tells us that we obtain two relatively prime integers when we divide each of two original integers by their greatest common divisor.

Theorem 3.6. If a and b be integers with $(a, b) = d$, then $(a/d, b/d) = 1$. (In other words, a/d and b/d are relatively prime.)

Proof. Let a and b be integers with $(a, b) = d$. We will show that a/d and b/d have no common positive divisors other than 1. Assume that e is a positive integer such that $e \mid (a/d)$ and $e \mid (b/d)$. Then there are integers k and l with $a/d = ke$ and $b/d = le$, so that $a = dek$ and $b = del$. Hence, de is a common divisor of a and b. Because d is the greatest common divisor of a and b, $de \leq d$, so that e must be 1. Consequently, $(a/d, b/d) = 1$. ∎

A fraction p/q where $(p, q) = 1$ is said to be in *lowest terms*. The following corollary tells us that every fraction equals a fraction in lowest terms.

Corollary 3.6.1. If a and $b \neq 0$ are integers, then $a/b = p/q$ for some integers p and $q \neq 0$ where $(p, q) = 1$. ∎

Proof. Suppose that a and $b \neq 0$ are integers. Set $p = a/d$ and $q = b/d$ where $d = (a, b)$. Then $p/q = (a/d)/(b/d) = a/b$. Theorem 3.6 tells us that $(p, q) = 1$, proving the corollary.

We do not change the greatest common divisor of two integers when we add a multiple of one of the integers to the other. In Example 3.6, we showed that $(24, 84) = 12$. When we add any multiple of 24 to 84, the greatest common divisor of 24 and the resulting number is still 12. For example, since $2 \cdot 24 = 48$ and $(-3) \cdot 24 = -72$, we see that $(24, 84 + 48) = (24, 132) = 12$ and $(24, 84 + (-72)) = (24, 12) = 12$. The reason for this is that the common divisors of 24 and 84 are the same as the common divisors of 24 and the integer that results when a multiple of 24 is added to 84. The proof of the following theorem justifies this reasoning.

Theorem 3.7. Let a, b, and c be integers. Then $(a + cb, b) = (a, b)$.

Proof. Let a, b, and c be integers. We will show that the common divisors of a and b are exactly the same as the common divisors of $a + cb$ and b. This will show that $(a + cb, b) = (a, b)$. Let e be a common divisor of a and b. By Theorem 1.9, we see that $e \mid (a + cb)$, so that e is a common divisor of $a + cb$ and b. If f is a common divisor of $a + cb$ and b, then by Theorem 1.9, we see that f divides $(a + cb) - cb = a$, so that f is a common divisor of a and b. Hence, $(a + cb, b) = (a, b)$. ∎

We will show that the greatest common divisor of the integers a and b, not both 0, can be written as a sum of multiples of a and b. To phrase this more succinctly, we use the following definition.

Definition. If a and b are integers, then a *linear combination* of a and b is a sum of the form $ma + nb$, where both m and n are integers.

Example 3.7. What are the linear combinations $9m + 15n$, where m and n are both integers? Among these combinations are $-6 = 1 \cdot 9 + (-1) \cdot 15$; $-3 = (-2)9 + 1 \cdot 15$; $0 = 0 \cdot 9 + 0 \cdot 15$; $3 = 2 \cdot 9 + (-1) \cdot 15$; $6 = (-1) \cdot 9 + 1 \cdot 15$; and so on. It can be shown that the set of all linear combinations of 9 and 15 is the set $\{\ldots, -12, -9, -6, -3, 0, 3, 6, 9,$

12, . . .}, as the reader should verify after reading the proofs of the following two theorems. ◀

In Example 3.8, we found that $(9, 15) = 3$ appears as the smallest positive linear combination with integer coefficients of 9 and 15. This is no accident, as the following theorem demonstrates.

Theorem 3.8. The greatest common divisor of the integers a and b, not both 0, is the least positive integer that is a linear combination of a and b.

Proof. Let d be the least positive integer that is a linear combination of a and b. (There is a *least* such positive integer, using the well-ordering property, since at least one of two linear combinations $1 \cdot a + 0 \cdot b$ and $(-1)a + 0 \cdot b$, where $a \neq 0$, is positive.) We write

$$d = ma + nb, \tag{3.1}$$

where m and n are integers. We will show that $d \mid a$ and $d \mid b$.

By the division algorithm, we have

$$a = dq + r, \quad 0 \leq r < d.$$

From this equation and (3.1), we see that

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

This shows that the integer r is a linear combination of a and b. Because $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d \mid a$. In a similar manner, we can show that $d \mid b$.

We have shown that d, the least positive integer that is a linear combination of a and b, is a common divisor of a and b. What remains to be shown is that it is the *greatest common divisor* of a and b. To show this, all we need show is that any common divisor c of a and b must divide d, since any proper positive divisor of d is less than d. Because $d = ma + nb$, if $c \mid a$ and $c \mid b$, Theorem 1.9 tells us that $c \mid d$, so that $d \geq c$. This concludes the proof. ■

From Theorem 3.8, we immediately see that the greatest common divisor of two integers a and b can be written as a linear combination of these integers. (Note that the theorem tells us not only that (a, b) can be written as a linear combination of these numbers, but also that it is the least such positive integer. Because this is such an important fact, we state it explicitly as a corollary.

Corollary 3.8.1 ***Bezout's Theorem.*** If a and b are integers, then there are integers m and n such that $ma + nb = (a, b)$.

Corollary 3.8.1 is called Bezout's theorem after *Étienne Bézout,* a French mathematician of the eighteenth century who proved a more general result about polynomials. Even though this corollary is known as Bezout's theorem, it had been established for integers many years earlier by Claude Gaspar Bachet (see Chapter 13 for his biography). The equation $ma + nb = (a, b)$ is known as *Bezout's identity,* and any integers m and n

that solve this equation for given integers a and b are called *Bezout coefficients* or *Bezout numbers* of the pair of integers a and b.

Example 3.8. Note that $(4, 10) = 2$ because 1 and 2 are the only positive common divisors of 4 and 10. The equation $(-2) \cdot 4 + 1 \cdot 10 = 2$ shows that -2 and 1 are Bezout coefficients of 4 and 10. Because $8 \cdot 4 + (-3) \cdot 10 = 2$, we see that 8 and -3 are also Bezout coefficients of 4 and 10. In fact, there are infinitely many different Bezout coefficients for 4 and 10 because $-2 + 10t$ and $1 + (-4)t$ are Bezout coefficients of 4 and 10 for every integer t. ◀

Because we will often need to apply Corollary 3.8.1 in the case where a and b are relatively prime integers, we call out this special case as a second corollary of Theorem 3.8.

Corollary 3.8.2. The integers a and b are relatively prime integers if and only if there are integers m and n such that $ma + nb = 1$.

Proof. To prove this corollary, note that if a and b are relatively prime, then $(a, b) = 1$. Consequently, by Theorem 3.8, 1 is the least positive integer that is a linear combination of a and b. It follows that there are integers m and n such that $ma + nb = 1$. Conversely, if there are integers m and n with $ma + nb = 1$, then by Theorem 3.8, it immediately

ÉTIENNE BÉZOUT (1730–1783) was born in Nemours, France, where his father was a magistrate. His parents wanted him to follow in his father's footsteps. However, he was enticed to become a mathematician by reading the writings of the great mathematician Leonhard Euler. Bézout published a series of research papers beginning in 1756, including several on integration. 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 lead to a four-volume textbook completed in 1767. In 1768, Bézout was appointed examiner of the Corps d'Artillerie; he was promoted to higher positions in 1768 and in 1770. He is well known for his six-volume comprehensive textbook on mathematics published between 1770 and 1782. Bézout's textbooks were extremely popular. In particular, his textbooks were studied by several generations of students who hoped to enter the École Polytechnique, the famous engineering and science school founded in 1794. These 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 *Thèorie générale des equations algebriques*, 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 Bezoutian by the great English mathematician James Joseph Sylvester).

Bezout 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.

follows that $(a, b) = 1$. This follows because not both a and b are zero and 1 is clearly the least positive integer that is a linear combination of a and b. ∎

Theorem 3.8 is valuable: We can obtain results about the greatest common divisor of two integers using the fact that the greatest common divisor is the least positive linear combination of these integers. Having different representations of the greatest common divisor of two integers allows us to choose the one that is most useful for a particular purpose. This is illustrated in the proof of the following theorem.

Theorem 3.9. If a and b are positive integers, then the set of linear combinations of a and b is the set of integer multiples of (a, b).

Proof. Suppose that $d = (a, b)$. We first show that every linear combination of a and b must also be a multiple of d. First note that by the definition of greatest common divisor, we know that $d \mid a$ and $d \mid b$. Now every linear combination of a and b is of the form $ma + nb$, where m and n are integers. By Theorem 1.9, it follows that whenever m and m are integers, d divides $ma + nb$. That is, $ma + nb$ is a multiple of d.

We now show that every multiple of d is also a linear combination of a and b. By Theorem 3.8, we know that there are integers r and s such that $(a, b) = ra + sb$. The multiples of d are the integers of the form jd, where j is an integer. Multiplying both sides of the equation $d = ra + sb$ by j, we see that $jd = (jr)a + (js)b$. Consequently, every multiple of d is a linear combination of a and b. This completes the proof. ∎

We have defined greatest common divisors using the notion that the integers are ordered. That is, given two distinct integers, one is larger than the other. However, we can define the greatest common divisor of two integers without relying on this notion of order, as we do in Theorem 3.10. This characterization of the greatest common divisor of two integers not depending on ordering is generalized in the study of algebraic number theory to apply to what are known as algebraic number fields.

Theorem 3.10. If a and b are integers, not both 0, then a positive integer d is the greatest common divisor of a and b if and only if

(i) $d \mid a$ and $d \mid b$, and

(ii) if c is an integer with $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. We will first show that the greatest common divisor of a and b has these two properties. Suppose that $d = (a, b)$. By the definition of common divisor, we know that $d \mid a$ and $d \mid b$. By Theorem 3.8, we know that $d = ma + nb$, where m and n are integers. Consequently, if $c \mid a$ and $c \mid b$, then by Theorem 1.9, $c \mid d = ma + nb$. We have now shown that if $d = (a, b)$, then properties (i) and (ii) hold.

Now assume that properties (i) and (ii) hold. Then we know that d is a common divisor of a and b. Furthermore, by property (ii), we know that if c is a common divisor of a and b, then $c \mid d$, so that $d = ck$ for some integer k. Hence, $c = d/k \leq d$. (We have used the fact that a positive integer divided by any nonzero integer is less than that integer.) This shows that a positive integer satisfying (i) and (ii) must be the greatest common divisor of a and b. ∎

Note that Theorem 3.10 tells us that the greatest common divisor of two integers a and b, not both 0, is the positive common divisor of these integers that is divisible by all other common divisors.

We have shown that the greatest common divisor of a and b, not both 0, is a linear combination of a and b. However, we have not explained how to find a particular linear combination of a and b that equals (a, b). In the next section, we will provide an algorithm that finds a particular linear combination of a and b that equals (a, b).

We can also define the greatest common divisor of more than two integers.

Definition. Let $a_1, a_2, \ldots, a_n$ be integers, not all 0. The *greatest common divisor* of these integers is the largest integer that is a divisor of all of the integers in the set. The greatest common divisor of $a_1, a_2, \ldots, a_n$ is denoted by $(a_1, a_2, \ldots, a_n)$. (Note that the order in which the a_i's appear does not affect the result.)

Example 3.9. We easily see that $(12, 18, 30) = 6$ and $(10, 15, 25) = 5$. ◀

We can use the following lemma to find the greatest common divisor of a set of more than two integers.

Lemma 3.2. If $a_1, a_2, \ldots, a_n$ are integers, not all 0, then $(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$.

Proof. Any common divisor of the n integers $a_1, a_2, \ldots, a_{n-1}, a_n$ is, in particular, a divisor of a_{n-1} and a_n, and therefore a divisor of (a_{n-1}, a_n). Also, any common divisor of the $n - 1$ integers $a_1, a_2, \ldots, a_{n-2}$, and (a_{n-1}, a_n) must be a common divisor of all n integers, for if it divides (a_{n-1}, a_n), then it must divide both a_{n-1} and a_n. Because the set of n integers and the set of the first $n - 2$ integers together with the greatest common divisor of the last two integers have exactly the same divisors, their greatest common divisors are equal. ■

Example 3.10. To find the greatest common divisor of the three integers 105, 140, and 350, we use Lemma 3.2 to see that $(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35$. ◀

Example 3.11. Consider the integers 15, 21, and 35. We find that the greatest common divisor of these three integers is 1 using the following steps:

$$(15, 21, 35) = (15, (21, 35)) = (15, 7) = 1.$$

Each pair among these integers has a common factor greater than 1, because $(15, 21) = 3$, $(15, 35) = 5$, and $(21, 35) = 7$. ◀

Example 3.11 motivates the following definition.

Definition. We say that the integers $a_1, a_2, \ldots, a_n$ are *mutually relatively prime* if $(a_1, a_2, \ldots, a_n) = 1$. These integers are called *pairwise relatively prime* if, for each pair

of integers a_i and a_j with $i \neq j$ from the set, $(a_i, a_j) = 1$; that is, if each pair of integers from the set is relatively prime.

The concept of pairwise relatively prime is used much more often than the concept of mutually relatively prime. Also, note that pairwise relatively prime integers must be mutually relatively prime, but that the converse is false (as the integers 15, 21, and 35 in Example 3.11 show).

3.3 Exercises

1. Find the greatest common divisor of each of the following pairs of integers.
a) 15, 35 c) -12, 18 e) 11, 121
b) 0, 111 d) 99, 100 f) 100, 102

2. Find the greatest common divisor of each of the following pairs of integers.
a) 5, 15 c) -27, -45 e) 100, 121
b) 0, 100 d) -90, 100 f) 1001, 289

3. Let a be a positive integer. What is the greatest common divisor of a and $2a$?

4. Let a be a positive integer. What is the greatest common divisor of a and a^2?

5. Let a be a positive integer. What is the greatest common divisor of a and $a + 1$?

6. Let a be a positive integer. What is the greatest common divisor of a and $a + 2$?

7. Show that the greatest common divisor of two even numbers is even.

8. Show that the greatest common divisor of an even number and an odd number is odd.

9. Show that if a and b are integers, not both 0, and c is a nonzero integer, then $(ca, cb) = |c|(a, b)$.

10. Show that if a and b are integers with $(a, b) = 1$, then $(a + b, a - b) = 1$ or 2.

11. What is $(a^2 + b^2, a + b)$, where a and b are relatively prime integers that are not both 0?

12. Show that if a and b are both even integers that are not both 0, then $(a, b) = 2(a/2, b/2)$.

13. Show that if a is an even integer and b is an odd integer, then $(a, b) = (a/2, b)$.

14. Show that if a, b, and c are integers such that $(a, b) = 1$ and $c \mid (a + b)$, then $(c, a) = (c, b) = 1$.

15. Show that if a, b, and c are mutually relatively prime nonzero integers, then $(a, bc) = (a, b)(a, c)$.

➢ **16.** a) Show that if a, b, and c are integers with $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.
b) Use mathematical induction to show that if $a_1, a_2, \ldots, a_n$ are integers, and b is another integer such that $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$, then $(a_1 a_2 \cdots a_n, b) = 1$.

17. Find a set of three integers that are mutually relatively prime, but any two of which are not relatively prime. Do not use examples from the text.

18. Find four integers that are mutually relatively prime such that any three of these integers are not mutually relatively prime.