Introduction

Elementary number theory is essentially the study of the system of integers. The system of integers consists of the set of integers $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and various properties of this set under the operations of addition and multiplication and under the usual ordering relation of "less than." These important properties of the integers are summarized below.

Closure property of addition: If $a, b \in \mathbf{Z}$, then $a + b \in \mathbf{Z}$.
Closure property of multiplication: If $a, b \in \mathbf{Z}$, then $ab \in \mathbf{Z}$.

Commutative property of addition: If $a, b \in \mathbf{Z}$, then $a + b = b + a$.
Commutative property of multiplication: If $a, b \in \mathbf{Z}$, then $ab = ba$.

Associative property of addition: If $a, b, c \in \mathbf{Z}$, then $(a + b) + c = a + (b + c)$.
Associative property of multiplication: If $a, b, c \in \mathbf{Z}$, then $(ab)c = a(bc)$.

Distributive property of multiplication over addition: If $a, b, c \in \mathbf{Z}$, then $a(b + c) = ab + ac$.

Additive identity property: If $a \in \mathbf{Z}$, then $a + 0 = 0 + a = a$.
Multiplicative identity property: If $a \in \mathbf{Z}$, then $a \cdot 1 = 1 \cdot a = a$.

Additive inverse property: If $a \in \mathbf{Z}$, then $a + (-a) = (-a) + a = 0$. If $a, b \in \mathbf{Z}$, then $a + (-b)$ is written $a - b$.

Zero property of multiplication: If $a \in \mathbf{Z}$, then $a \cdot 0 = 0 \cdot a = 0$.

Cancellation property of addition: If $a, b, c \in \mathbf{Z}$ and $a + b = a + c$, then $b = c$.
Cancellation property of multiplication: If $a, b, c \in \mathbf{Z}, a \neq 0$, and $ab = ac$, then $b = c$.

Trichotomy law: If $a \in \mathbf{Z}$, then exactly one of the following statements is true:
(i) $a < 0$
(ii) $a = 0$
(iii) $a > 0$

Properties of inequality:
(i) If $a, b, c \in \mathbf{Z}$ and $a < b$, then $a + c < b + c$.
(ii) If $a, b, c \in \mathbf{Z}$, $a < b$, and $c > 0$, then $ac < bc$.
(iii) If $a, b, c \in \mathbf{Z}$, $a < b$, and $c < 0$, then $ac > bc$.

Well-ordering property: Every nonempty set of positive integers contains a least element.

We hope that you are familiar, or at least comfortable, with these properties as a result of your past encounters with ordinary arithmetic. The properties above are taken as axioms of the system of integers in this book. These axioms are not independent; in other words, it is possible to prove some of the axioms from others. A rigorous development of the system of integers may be found in Fletcher and Patty (1992).

The well-ordering property is a fundamentally important axiom of the system of integers above. One powerful proof technique available to the number theorist (indeed, any mathematician) is that of *mathematical induction*. A review of the two essential forms of mathematical induction, called the first and second principles, may be found in Appendix A along with a few exercises and an appropriate reference. Both of these principles of mathematical induction are logically equivalent to the well-ordering principle. So, by accepting the well-ordering principle as an axiom of the system of integers, we obtain two forms of induction for our use. Mathematical induction will be used frequently in this book, especially in Chapter 7.

This short introductory chapter concludes by establishing the framework of the remainder of this book. Throughout, the results are labeled with a variety of terms: proposition, theorem, lemma, corollary, and porism. For the meanings of the terms and further explanation, refer to the Preface to the Student. More globally, mathematics breaks roughly into two disciplines: The *pure* discipline of mathematics is concerned primarily with theory, while the *applied* discipline is concerned primarily with applications. These disciplines within mathematics do not have clear-cut boundaries; indeed, there is much theory in applied mathematics and there are frequently many applications in pure mathematics. Elementary number theory falls into the pure discipline of mathematics. Elementary number theory does, however, have applications in other fields. One such field is computer science. The importance of computer science applications in today's technological world cannot be overemphasized. An excellent reference for applications of elementary number theory in computer science is Knuth (1981). (See also Student Project 7 in Chapter 8.) Another field based on the principles of elementary number theory is cryptography, the making and breaking of secret codes. A particular cryptographic system is discussed in Section 8.2. An excellent reference for cryptographic applications of elementary number theory is Konheim (1981).

1

Divisibility and Factorization

Elementary number theory is the study of the divisibility properties of the integers. Inasmuch as these divisibility properties form the basis for the study of more advanced topics in number theory, they can be thought of as forming the foundation for the entire area of number theory. It is both beautiful and appropriate that such a pure area of mathematics is derived from such a simple source. In addition, the main topics of this chapter are quite old, dating back to the Alexandrian Greek period of mathematics, which began approximately 300 B.C. In fact, most of the ideas discussed here appear in Euclid's *Elements.*

In this chapter, we develop the concept of divisibility and the related concept of factorization, which culminate in an extremely important property of the integers appropriately named the Fundamental Theorem of Arithmetic. In addition, we will encounter and highlight certain proof strategies that are used again and again in elementary number theory. These strategies form some of the important "tools of the trade" of the number theorist.

1.1 Divisibility

The fundamental relation connecting one integer to another is the notion of divisibility. In terms of long division, the divisibility relation means "divides evenly with zero remainder." Hence, the integer 3 divides the integer 6 since 3 divides evenly into 6 (two times) with zero remainder. Similarly, the integer 3 does not divide the integer 5, since 3 does not divide evenly into 5; 3 divides into 5 with a quotient of 1 and a remainder of 2. We now make the divisibility relation more mathematically precise.

Biography

Euclid of Alexandria (365?–275? B.C.)

Little is known of Euclid's life. The exact dates of his birth and death (as well as his birthplace and nationality) are unknown. Euclid is remembered mainly for his monumental work, entitled *Elements*, which was essentially a compilation of the mathematics of the classical Greek period that preceded him. This massive work comprised 13 books and contained 465 propositions. *Elements* emphasized the discipline of mathematics as a deductive science based on explicit axioms and, as such, has influenced the course of mathematics as has no other work. While much of *Elements* was devoted to geometry, Books VII–IX as well as portions of Book X were devoted to the theory of numbers. It is Euclid's proof of the infinitude of the prime numbers that is still used today. In addition, Euclid studied the division algorithm (culminating in the so-called Euclidean algorithm for the computation of greatest common divisors), perfect numbers, and Pythagorean triples. (All of the number-theoretic topics above will be discussed in this book.)

Definition 1: Let $a, b \in \mathbf{Z}$. Then *a divides b*, denoted $a \mid b$, if there exists $c \in \mathbf{Z}$ such that $b = ac$. If $a \mid b$, then a is said to be a *divisor* or *factor* of b. The notation $a \nmid b$ means that a does not divide b.

Example 1:

(a) $3 \mid 6$ since there exists $c \in \mathbf{Z}$ such that $6 = 3c$. Here, $c = 2$. Hence 3 is a divisor of 6.

(b) $3 \nmid 5$ since there does not exist $c \in \mathbf{Z}$ such that $5 = 3c$. Note that c would have to be $\frac{5}{3}$ here and $\frac{5}{3} \notin \mathbf{Z}$. Hence 3 is not a divisor of 5.

(c) $3 \mid -6$ since there exists $c \in \mathbf{Z}$ such that $-6 = 3c$. Here, $c = -2$. Hence 3 is a divisor of -6. In fact, it is easily seen that $\pm 3 \mid \pm 6$.

(d) If $a \in \mathbf{Z}$, then $a \mid 0$ since there exists $c \in \mathbf{Z}$ such that $0 = ac$. Here, $c = 0$. In other words, any integer divides 0.

(e) If $a \in \mathbf{Z}$ and $0 \mid a$, then there exists $c \in \mathbf{Z}$ such that $a = 0c$ if and only if $a = 0$. In other words, the only integer having zero as a divisor is zero.

We now make two remarks concerning the notation $a \mid b$. First of all, $a \mid b$ does not have the same meaning as either of the notations a/b and b/a. Note that $a \mid b$ is a statement about the relationship between two integers: It says that a divides into b evenly with no remainder. The notations a/b and b/a are interpreted, respectively, as $a \div b$ and $b \div a$ and, as such, are rational numbers. In other words, $a \mid b$ is a statement *about* numbers while a/b and b/a *are* numbers. Note, however, that $a \mid b$ does imply that a divides b exactly b/a times provided that $a \neq 0$.

The restriction that a not be zero in the implication above brings us to our second remark. You may feel uncomfortable about allowing zero as a divisor in (e) of Example 1 above. The phrase "division by zero is undefined" has probably been ingrained in your mind through constant repetition by many of your mathematics teachers. We say that $0 \mid 0$ here only because it is consistent with our definition of divisibility; it should not be interpreted as implying that 0 divides 0 exactly 0/0 times. The form 0/0 is said to be *indeterminate*: It has no meaning. The difference between the notation $0 \mid 0$ and 0/0 is hence clear—the former notation has meaning (albeit minimal and only as a consequence of our definition), and the latter notation does not have meaning. We urge the reader to pause and carefully consider the remarks above before continuing.

The divisibility relation enjoys the following two properties, which are recorded as propositions.

Proposition 1.1: Let $a, b, c \in \mathbf{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Since $a \mid b$ and $b \mid c$, there exist $e, f \in \mathbf{Z}$ such that $b = ae$ and $c = bf$. Then

$$c = bf = (ae)f = a(ef)$$

and $a \mid c$. ■

Before continuing, note that we have just proven that the divisibility relation is transitive. If the word *transitive* is unfamiliar to you, see Appendix B [in particular, Example 3(b)] for a further discussion of relations and their properties.

Proposition 1.2: Let $a, b, c, m, n \in \mathbf{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid ma + nb$.

Proof: Since $c \mid a$ and $c \mid b$, there exist $e, f \in \mathbf{Z}$ such that $a = ce$ and $b = cf$. Then

$$ma + nb = mce + ncf = c(me + nf)$$

and $c \mid ma + nb$. ■

A special case of Proposition 1.2 is important enough to be highlighted separately. We first give a special name to the expression $ma + nb$.

Definition 2: The expression $ma + nb$ in Proposition 1.2 is said to be an *integral linear combination* of a and b.

Proposition 1.2 says that an integer dividing each of two integers also divides any integral linear combination of those integers. This fact is extremely valuable in establishing theoretical results. Consider the special case where $m = n = 1$. We obtain the fact that, if an integer divides each of two integers, then it divides the sum of the integers. The case where $m = 1$ and $n = -1$ similarly yields the fact that, if an integer divides each of two integers, then it divides the difference of the two integers. We will use these facts repeatedly in this book, and you will find them particularly useful in several theoretical exercises.

We now introduce a function with the set of real numbers $\mathbf{R}$ as its domain and the set of integers $\mathbf{Z}$ as its range. This function will be used shortly to prove the major result on divisibility; it will also be useful in Chapters 4 and 7.

Definition 3: Let $x \in \mathbf{R}$. The *greatest integer function of x,* denoted $[x]$, is the greatest integer less than or equal to x.

The existence of a greatest integer less than or equal to a given real number follows from the well-ordering property of the integers discussed in the Introduction.

Example 2:

(a) If $a \in \mathbf{Z}$, then $[a] = a$ since the greatest integer less than or equal to any integer is the integer itself. It is easily seen that the converse of this statement is also true, namely that, if $[a] = a$ for some $a \in \mathbf{R}$, then $a \in \mathbf{Z}$.

(b) Since the greatest integer less than or equal to $\frac{5}{3}$ is 1, we have $[\frac{5}{3}] = 1$.

(c) Since the greatest integer less than or equal to π is 3, we have $[\pi] = 3$.

(d) Since the greatest integer less than or equal to $-\frac{5}{3}$ is -2, we have $[-\frac{5}{3}] = -2$.

(e) Since the greatest integer less than or equal to $-\pi$ is -4, we have $[-\pi] = -4$.

The following lemma is basically an immediate consequence of the definition of the greatest integer function, but a short proof is nonetheless provided for your inspection.

Lemma 1.3: Let $x \in \mathbf{R}$. Then $x - 1 < [x] \leq x$.

Proof: Since the greatest integer function of x is less than or equal to x, the second inequality is clear. For the first inequality, assume, by way of contradiction, that $x - 1 \geq [x]$. Then $[x] + 1 \leq x$ and

$$[x] < [x] + 1 \leq x$$

$$\begin{array}{rl}
 & 1 \leftarrow \text{Quotient} \\
\text{Divisor} \rightarrow 3 & \overline{)5} \leftarrow \text{Dividend} \\
 & \underline{-3} \\
 & 2 \leftarrow \text{Remainder}
\end{array}$$

Figure 1.1

Since $[x] + 1$ is an integer, this contradicts the fact that $[x]$ is the greatest integer less than or equal to x. Hence $x - 1 < [x]$. ■

When one integer (the divisor) is divided into another integer (the dividend) to obtain an integer quotient, an integer remainder is obtained. For example, the long division for 3 divided into 5 (shown in Figure 1.1) can be expressed more compactly via the equation

$$5 = 3 \cdot 1 + 2$$

or by the phrase "the dividend is equal to the divisor times the quotient plus the remainder." Note that the remainder is strictly less than the divisor. If the divisor in such a long division of integers is positive, the fact above is true in general as the following theorem illustrates.

Theorem 1.4: (The Division Algorithm) Let $a, b \in \mathbf{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbf{Z}$ such that

$$a = bq + r, \qquad 0 \leq r < b$$

(Note that q stands for *quotient* and r stands for *remainder.*)

Proof: Let $q = \left[\frac{a}{b}\right]$ and $r = a - b\left[\frac{a}{b}\right]$. Then $a = bq + r$ is easily checked. It remains to show that $0 \leq r < b$. By Lemma 1.3, we have that

$$\frac{a}{b} - 1 < \left[\frac{a}{b}\right] \leq \frac{a}{b}$$

Multiplying all terms of this inequality by $-b$, we obtain

$$b - a > -b\left[\frac{a}{b}\right] \geq -a$$

Reversing the inequality and adding a to all terms gives

$$0 \leq a - b\left[\frac{a}{b}\right] < b$$

which is precisely $0 \leq r < b$ as desired; so, q and r as defined above have the desired properties. It remains to show the uniqueness of q and r. Assume that

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2, \qquad 0 \leq r_2 < b$$

We must show that $q_1 = q_2$ and $r_1 = r_2$. We have

$$0 = a - a = bq_1 + r_1 - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2)$$

which implies that

$$r_2 - r_1 = b(q_1 - q_2) \tag{1}$$

Hence, $b \mid r_2 - r_1$. Now $0 \le r_1 < b$ and $0 \le r_2 < b$ imply $-b < r_2 - r_1 < b$; along with $b \mid r_2 - r_1$, we have $r_2 - r_1 = 0$ or $r_1 = r_2$. Now (1) becomes

$$0 = b(q_1 - q_2)$$

Since $b \neq 0$, we have that $q_1 - q_2 = 0$ or $q_1 = q_2$ as desired. ■

Note that $r = 0$ in the division algorithm if and only if $b \mid a$. Equivalently, a necessary and sufficient condition in Theorem 1.4 for the remainder in a division of integers to be zero is that the divisor evenly divide the dividend.

Given $a, b \in \mathbf{Z}$ with $b > 0$, the q and r of the division algorithm may be obtained by using the equations defining q and r in the first statement of the proof of the algorithm. (In fact, one would use precisely these equations to compute q and r on a standard calculator.) We illustrate with an example.

Example 3:

Find q and r as in the division algorithm if $a = -5$ and $b = 3$.
By the proof of Theorem 1.4, we have

$$q = \left[\frac{a}{b}\right] = \left[\frac{-5}{3}\right] = -2$$

and

$$r = a - b\left[\frac{a}{b}\right] = -5 - 3(-2) = 1$$

Please check for yourself that $a = bq + r$ and $0 \le r < b$.

A remark is in order here. When asked, "What is -5 divided by 3?" (as in Example 3 above), many students will respond "-1 with a remainder of -2" since $-\frac{5}{3} = -1 - \frac{2}{3}$. Although $q = -1$ and $r = -2$ satisfy $a = bq + r$, the condition that $0 \le r < b$ in Theorem 1.4 is no longer true. Hence, division in the context of the division algorithm must be performed carefully so that both desired conditions hold. More generalized versions of Theorem 1.4 that allow negative divisors are investigated in Exercise 15.

We conclude this section with a definition and an example of concepts with which you are probably already familiar.

Definition 4: Let $n \in \mathbf{Z}$. Then n is said to be *even* if $2 \mid n$ and n is said to be *odd* if $2 \nmid n$.

Example 4:

The set of even integers is given by $\{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$; the set of odd integers is given by $\{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\}$.

Exercise 11 establishes important facts about even and odd integers that will be useful throughout this book; solving this exercise is greatly encouraged.

Exercise Set 1.1

1. Prove or disprove each statement below.
   (a) $6 \mid 42$
   (b) $4 \mid 50$
   (c) $16 \mid 0$
   (d) $0 \mid 15$
   (e) $14 \mid 997157$
   (f) $17 \mid 998189$
2. Find integers a, b, and c such that $a \mid bc$ but $a \nmid b$ and $a \nmid c$.
3. Find the unique integers q and r guaranteed by the division algorithm (Theorem 1.4) with each dividend and divisor below.
   (a) $a = 47$, $b = 6$
   (b) $a = 281$, $b = 13$
   (c) $a = 343$, $b = 49$
   (d) $a = -105$, $b = 10$
   (e) $a = -469$, $b = 31$
   (f) $a = -500$, $b = 28$
4. If $a, b \in \mathbf{Z}$, find a necessary and sufficient condition that $a \mid b$ and $b \mid a$.
5. Prove or disprove the following statements.
   (a) If a, b, c, and d are integers such that $a \mid b$ and $c \mid d$, then $a + c \mid b + d$.
   (b) If a, b, c, and d are integers such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.
   (c) If a, b, and c are integers such that $a \nmid b$ and $b \nmid c$, then $a \nmid c$.
6. *(a)* Let $a, b, c \in \mathbf{Z}$ with $c \neq 0$. Prove that $a \mid b$ if and only if $ac \mid bc$.
   (b) Provide a counterexample to show why the statement of part (a) does not hold if $c = 0$.
7. Let $a, b \in \mathbf{Z}$ with $a \mid b$. Prove that $a^n \mid b^n$ for every positive integer n.
8. Let $n \in \mathbf{Z}$ with $n > 0$. Prove that $n \mid (n + 1)^n - 1$.
9. Let a, m and n be positive integers with $a > 1$. Prove that $a^m - 1 \mid a^n - 1$ if and only if $m \mid n$. [*Hint*: For the "if" direction, write $n = md$ with d a positive integer and use the factorization $a^{md} - 1 = (a^m - 1) \times (a^{m(d-1)} + a^{m(d-2)} + \cdots + a^m + 1)$.]
10. *(a)* Let $n \in \mathbf{Z}$. Prove that $3 \mid n^3 - n$.
   (b) Let $n \in \mathbf{Z}$. Prove that $5 \mid n^5 - n$.
   (c) Let $n \in \mathbf{Z}$. Is it true that $4 \mid n^4 - n$? Provide a proof or counterexample.
11. *(a)* Let $n \in \mathbf{Z}$. Prove that n is an even integer if and only if $n = 2m$ with $m \in \mathbf{Z}$.
   ✓
   (b) Let $n \in \mathbf{Z}$. Prove that n is an odd integer if and only if $n = 2m + 1$ with $m \in \mathbf{Z}$.
   (c) Prove that the sum and product of two even integers are even.
   (d) Prove that the sum of two odd integers is even and that their product is odd.

(e) Prove that the sum of an even integer and an odd integer is odd and that their product is even.

12. Prove that the square of any odd integer is expressible in the form $8n + 1$ with $n \in \mathbf{Z}$.

13. Prove that the fourth power of any odd integer is expressible in the form $16n + 1$ with $n \in \mathbf{Z}$.

14. *(a)* Let x be a positive real number and let d be a positive integer. Prove that the number of positive integers less than or equal to x that are divisible by d is $\left[\frac{x}{d}\right]$.

(b) Find the number of positive integers not exceeding 500 that are divisible by 3.

(c) Find the number of positive integers between 200 and 500 that are divisible by 3.

15. [The following exercise presents two alternate versions of the division algorithm (Theorem 1.4). Both versions allow negative divisors; as such, they are more general than Theorem 1.4.]

(a) Let a and b be nonzero integers. Prove that there exist unique $q, r \in \mathbf{Z}$ such that

$$a = bq + r, \qquad 0 \leq r < |b|$$

(b) Find the unique q and r guaranteed by the division algorithm of part (a) above with $a = 47$ and $b = -6$.

(c) Let a and b be nonzero integers. Prove that there exist unique $q, r \in \mathbf{Z}$ such that

$$a = bq + r, \qquad -\frac{|b|}{2} < r \leq \frac{|b|}{2}$$

This algorithm is called the *absolute least remainder algorithm.*

(d) Find the unique q and r guaranteed by the division algorithm of part (c) above with $a = 47$ and $b = -6$.

1.2

Prime Numbers

Every integer greater than one has at least two positive divisors, namely, 1 and the integer itself. Those positive integers having no other positive divisors (and so exactly two positive divisors) are of crucial importance in number theory and are introduced now.

Definition 5: Let $p \in \mathbf{Z}$ with $p > 1$. Then p is said to be *prime* if the only positive divisors of p are 1 and p. If $n \in \mathbf{Z}$, $n > 1$, and n is not prime, then n is said to be *composite.*

Note that the positive integer 1 is neither prime nor composite by definition. The reason for disallowing 1 as a prime number is investigated in Exercise 66.

Example 5:

The prime numbers between 2 and 50 inclusive are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47. Exercise 22 shows that all prime numbers except the integer 2 are odd and hence the integer 2 is the only even prime number.

Having introduced the concept of a prime number, a most fundamental question arises. Are there finitely many or infinitely many prime numbers? Before reading further, formulate your own conjecture; Theorem 1.6 will ultimately provide the answer to this question. We first prove a preliminary lemma.

Lemma 1.5: Every integer greater than 1 has a prime divisor.

Proof: Assume, by way of contradiction, that some integer greater than 1, say n, has no prime divisor. By the well-ordering property, we may assume that n is the least such integer. Now $n \mid n$; since n has no prime divisor, n is not prime. So n is composite and consequently there exist $a, b \in \mathbf{Z}$ such that $n = ab$, $1 < a < n$, and $1 < b < n$. Since $1 < a < n$, we have that a has a prime divisor, say p, so that $p \mid a$. But $a \mid n$ so we have that $p \mid n$ by Proposition 1.1 from which n has a prime divisor, a contradiction. So every integer greater than 1 has a prime divisor. ■

We may now answer our motivating question posed prior to Lemma 1.5. This result appears as Proposition 20 in Book IX of Euclid's *Elements*; study the proof carefully because it is a vivid illustration of great mathematical ingenuity.

Theorem 1.6: (Euclid) There are infinitely many prime numbers.

Proof: Assume, by way of contradiction, that there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$. Now N has a prime divisor, say p, by Lemma 1.5. So $p = p_i$ for some i, $i = 1, 2, \ldots, n$. Then $p \mid N - p_1 p_2 \cdots p_n$ (by Proposition 1.2), which implies that $p \mid 1$, a contradiction. Hence, there are infinitely many prime numbers. ■

The point of ingenuity in the proof above is the construction of the number N; it is precisely consideration of this number that eventually results in the desired contradiction. You will find similar constructions useful throughout this book.

Given that there are infinitely many prime numbers, how can we go about finding these numbers? The following proposition is useful in this regard.

Proposition 1.7: Let n be a composite number. Then n has a prime divisor p with $p \leq \sqrt{n}$.

Proof: Since n is a composite number, there exist $a, b \in \mathbf{Z}$ such that $n = ab$, $1 < a < n$, $1 < b < n$, and, without loss of generality, $a \leq b$. Now $a \leq \sqrt{n}$. (If $a > \sqrt{n}$, we have

$$n = ab > \sqrt{n}\sqrt{n} = n$$

which is impossible.) By Lemma 1.5, we have that a has a prime divisor, say p, so that $p \mid a$. But $a \mid n$, so we have that $p \mid n$ by Proposition 1.1. Furthermore, $p \leq a \leq \sqrt{n}$; p is the desired prime divisor of n. ■

Proposition 1.7 yields a method for finding all prime numbers less than or equal to a specified integer $n > 1$ by producing a criterion satisfied by all composite numbers. If an integer greater than one fails to satisfy this criterion, then the integer cannot be composite and so is prime. This method is called the *sieve of Eratosthenes* and is one of several "sieve methods." We illustrate the sieve of Eratosthenes with an example.

Example 6:

Suppose that we wish to find all prime numbers less than or equal to 50. By Proposition 1.7, any composite number less than or equal to 50 must have a prime divisor less than or equal to $\sqrt{50} \approx 7.07$. The prime numbers less than or equal to 7.07 are 2, 3, 5, and 7. Hence, from a list of the integers from 2 to 50, we delete all multiples of 2, all multiples of 3, all multiples of 5, and all multiples of 7 (not including 2, 3, 5, and 7 themselves). Note that all such multiples are clearly composite.

	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~~

Any number remaining in the list is not divisible by 2, 3, 5, or 7 and, by Proposition 1.7, cannot be composite. So the numbers remaining in the list above are prime (compare these numbers with those in Example 5); the composite numbers have been "sieved out" of the list.

In addition to finding prime numbers, Proposition 1.7 can be used to determine an algorithm for testing whether a given positive integer $n > 1$ is prime or composite. One checks whether n is divisible by any prime number p with $p \leq \sqrt{n}$. If it is divisible, then n is composite; if not, then n is prime. Such an algorithm is an example of a *primality test.* Note that this particular primality test is highly inefficient since it requires testing a given integer for divisibility by all prime numbers less than or equal to the square root of the integer. More useful primality testing algorithms exist — unfortunately, they require more number theory than we have developed at the present time. Two such primality tests are discussed in Section 8.3. The largest prime number known at this writing was discovered in 1999: $2^{6972593} - 1$. We will return to this prime number later. In addition, the primality or compositeness of any given integer between 101 and 9999 inclusive may be deduced using the grid inside the cover of this book; instructions for using this grid may be found in Table 1 of Appendix E.

Biography

Eratosthenes of Cyrene (276–194 B.C.)

Eratosthenes, a contemporary of Archimedes, is perhaps best remembered as the chief librarian at the University of Alexandria in ancient Egypt. Born in Cyrene on the southern coast of the Mediterranean Sea, he was gifted not only as a mathematician, but also as a philosopher, astronomer, poet, historian, and athlete. There is much speculation as to his nickname of "Beta." One theory offers that the nickname originated from the fact that he stood at least second in each of the branches of knowledge of his day. In 240 B.C., Eratosthenes made what was perhaps his most significant scientific contribution when he measured the circumference of the earth using a simple application of Euclidean geometry. His primary contribution to number theory is his famous sieve for finding prime numbers as discussed in the text.

How are prime numbers distributed among the positive integers? A solution of Exercise 17 suggests that the prime numbers are distributed more sparsely as you progress through larger and larger positive integers. The proposition below shows more precisely that there exist arbitrarily long sequences of consecutive positive integers containing no prime numbers. Equivalently, there exist arbitrarily large gaps between prime numbers.

Proposition 1.8: For any positive integer n, there are at least n consecutive composite positive integers.

Proof: Given the positive integer n, consider the n consecutive positive integers

$$(n + 1)! + 2, (n + 1)! + 3, \dots, (n + 1)! + n + 1$$

Let i be a positive integer such that $2 \le i \le n + 1$. Since $i \mid (n + 1)!$ and $i \mid i$, we have

$$i \mid (n + 1)! + i, \qquad 2 \le i \le n + 1$$

by Proposition 1.2. So each of the n consecutive positive integers above is composite. ■

Example 7:

By the proof of Proposition 1.8 above, a sequence of eight consecutive composite positive integers is given by $9! + 2$, $9! + 3, \dots, 9! + 9$ or, equivalently, 362882, 362883, . . . , 362889. Note that there is no guarantee that the sequence of integers produced by the proof of Proposition 1.8 will be the least such occurrence of integers. For example, the least occurrence of eight consecutive composite positive integers is given by the sequence 114, 115, 116, 117, 118, 119, 120, and 121.

Since 2 is the only even prime number, the only consecutive prime numbers are 2 and 3. How many pairs of prime numbers differ by two as in 3 and 5, 5 and 7, 11 and 13, and so on? Such pairs of prime numbers are said to be *twin primes*. Unfortunately, the answer to this question is unknown. The operative conjecture asserts the existence of infinitely many twin primes, as stated below.

Conjecture 1: (Twin Prime Conjecture) There are infinitely many prime numbers p for which $p + 2$ is also a prime number.

The largest known pair of twin primes is $318032361 \cdot 2^{107001} \pm 1$, discovered in 2001 by D. Underbakke and P. Carmody.

The most famous result concerning the distribution of prime numbers is called the Prime Number Theorem. This theorem was conjectured in 1793 by Carl Friedrich Gauss but resisted proof until 1896 when two independent proofs were produced by J. Hadamard and C. J. de la Vallée Poussin. The Prime Number Theorem gives an estimate of the number of prime numbers less than or equal to a given positive real number x. The estimate improves as x gets large. We first define a function that counts prime numbers.

Definition 6: Let $x \in \mathbf{R}$ with $x > 0$. Then $\pi(x)$ is the function defined by

$$\pi(x) = |\{p : p \text{ prime}; 1 < p \leq x\}|$$

In this book, vertical bars enclosing a set (as in Definition 6 above) will denote the cardinality of the set. So, if x is a positive real number, then $\pi(x)$ is the number of prime numbers less than or equal to x.

Example 8:

From Example 5, we have that the number of prime numbers less than or equal to 50 is 15. So $\pi(50) = 15$.

We may now state the Prime Number Theorem.

Theorem 1.9: (Prime Number Theorem) $\displaystyle\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1.$

The Prime Number Theorem says that, for large x, the quantity $\frac{\pi(x) \ln x}{x}$ is close to 1. This is equivalent to saying that the quantity $\pi(x)$ may be approximated by $\frac{x}{\ln x}$. In other words, $\frac{x}{\ln x}$ is an estimate for $\pi(x)$ for large x. Table 1.1 gives a

Table 1.1

x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{\pi(x)\ln x}{x}$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78498	72382.4	1.084
10^7	664579	620420.7	1.071
10^8	5761455	5428681.0	1.061

comparison of $\pi(x)$ and $\frac{x}{\ln x}$ for increasingly larger values of x. Note how the ratio $\frac{\pi(x)\ln x}{x}$ gets closer and closer to 1 as $x \to \infty$.

The most direct proof of the Prime Number Theorem requires considerable complex analysis, which is beyond the scope of this book. A complete discussion of this analytic proof may be found in Apostol (1976). In 1949, Atle Selberg and Paul Erdös discovered a surprising new proof of the Prime Number Theorem. This new proof was termed "elementary" by the mathematical community; although lengthy and considerably more intricate than the original proof, the new one is accessible to anyone with a knowledge of calculus. The elementary proof may be found in Hardy and Wright (1979).

Many unsolved problems in number theory deal with integers that are expressible in certain forms. One of the most famous unsolved problems in all of number theory was conjectured by Christian Goldbach in a letter to the great Leonhard Euler.

Conjecture 2: (Goldbach, 1742) Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.

As three quick illustrations of such expressions, consider $4 = 2 + 2$, $6 = 3 + 3$, and $8 = 3 + 5$. Goldbach's Conjecture (as Conjecture 2 has come to be known, appropriately enough) has been verified for all even integers less than $4 \cdot 10^{14}$. By experimentation with small even integers, the interested reader can discover that the representation of an even integer as the sum of two prime numbers may not be unique. (In fact, the number of such representations has been predicted in a formula by English mathematicians G. H. Hardy and J. E. Littlewood.) However, a proof that at least one such representation exists for every even integer greater than 2 remains elusive.

We conclude this section with a discussion of three unsolved problems concerning prime numbers expressible in certain forms and a related helpful remark for the exercises. The first form is named after a French monk, Father Marin Mersenne (1588–1648).

Definition 7: Any prime number expressible in the form $2^p - 1$ with p prime is said to be a *Mersenne prime*.

Example 9:

The first five Mersenne primes are 3 ($= 2^2 - 1$), 7 ($= 2^3 - 1$), 31 ($= 2^5 - 1$), 127 ($= 2^7 - 1$), and 8191 ($= 2^{13} - 1$). Note that $2^{11} - 1 = 2047 = (23)(89)$ is *not* a Mersenne prime.

In 1644, Mersenne authored *Cogitata Physica-Mathematica* in which he claimed that $2^p - 1$ was a prime number for p equal to 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257 and a composite number for all other prime numbers p with $p < 257$. Work completed in 1947 revealed that Mersenne made five mistakes: $2^p - 1$ is a prime number for p equal to 61, 89, and 107 (not included in Mersenne's list) and is a composite number for p equal to 67 and 257 (included in Mersenne's list). There are currently 38 known Mersenne primes. The largest known Mersenne prime is of vintage 1999 and was discovered by N. Hajratwala, G. Woltman, and S. Kurowski; it is $2^{6972593} - 1$, a number containing 2098960 digits. (The observant reader will recall that this Mersenne prime is also the largest known prime number!) Curiously enough, the Mersenne primes have *not* been discovered in increasing order. For example, the 31st known Mersenne prime, $2^{110503} - 1$, was discovered three years after the larger 30th known Mersenne prime, $2^{216091} - 1$. It may be that other Mersenne primes lie in the gaps formed by known Mersenne primes. In any event, most mathematicians believe that there are infinitely many Mersenne primes, and so we state the following conjecture.

Conjecture 3: There are infinitely many Mersenne primes.

The second form for prime numbers is named after French mathematician Pierre de Fermat.

Definition 8: Any prime number expressible in the form $2^{2^n} + 1$ with $n \in \mathbf{Z}$ and $n \geq 0$ is said to be a *Fermat prime*.

Example 10:

The first five Fermat primes are 3 ($= 2^{2^0} + 1$), 5 ($2^{2^1} + 1$), 17 ($= 2^{2^2} + 1$), 257 ($= 2^{2^3} + 1$), and 65537 ($= 2^{2^4} + 1$).

Fermat conjectured in 1640 that any number expressible in the form $2^{2^n} + 1$ with $n \in \mathbf{Z}$ and $n \geq 0$ is prime. The conjecture was disproved in 1732 by Euler, who proved that $641 \mid 2^{2^5} + 1$ and hence $2^{2^5} + 1$ is *not* a Fermat prime.

Currently, only five Fermat primes are known, namely those prime numbers given in Example 10 above. Many mathematicians believe that there are no Fermat primes other than these five; thus the following conjecture.

Conjecture 4: There are exactly five Fermat primes.

The final form for prime numbers that we examine here are those prime numbers that are expressible as one more than a perfect square. The conjecture below was made in 1922 by Hardy and Littlewood:

Conjecture 5: There are infinitely many prime numbers expressible in the form $n^2 + 1$ where n is a positive integer.

If you are interested, there are several examples of primes of the form in Conjecture 5.

We make one final remark here. In view of Conjecture 5 above, it may be tempting to conjecture that there are infinitely many prime numbers expressible in the form $n^2 - 1$ where n is a positive integer. This conjecture, however, is easily seen to be false. Note first that $n = 1$ does not give a prime number when substituted in the desired form, while $n = 2$ does. Now note that

$$n^2 - 1 = (n - 1)(n + 1)$$

Inasmuch as the product $(n - 1)(n + 1)$ gives a nontrivial factorization of $n^2 - 1$ if $n > 2$, we have the fact that $n^2 - 1$ is a prime number if and only if $n = 2$. Something as simple as factoring expressions can be a powerful tool in number theory (see also Exercise 9 of Section 1). Remember this tool!

Exercise Set 1.2

16. Determine whether the following positive integers are prime or composite by using the primality test motivated by Proposition 1.7.
(a) 127
(b) 129
(c) 131
(d) 133
(e) 137
(f) 139

17. Use the sieve of Eratosthenes to find all prime numbers less than 200.

18. *(a)* Find 13 consecutive composite positive integers.
(b) Find the least occurrence of 13 consecutive composite positive integers. (*Hint*: Use Table 3 in Appendix E.)

19. Find all twin primes less than 200.

20. *(a)* Find $\pi(10)$, $\pi(100)$, and $\pi(200)$.
(b) Compute $\frac{\pi(x)\ln x}{x}$ for $x = 10$, $x = 100$, and $x = 200$ and compare the obtained values with those in Table 1.1.

21. Verify Goldbach's Conjecture (Conjecture 2) for the following even integers.
(a) 30
(b) 98

(c) 114
(d) 222

22. Prove that 2 is the only even prime number.
23. Prove or disprove the following conjecture, which is similar to Conjecture 1.
    Conjecture: There are infinitely many prime numbers p for which $p + 2$ and $p + 4$ are also prime numbers.
24. Prove that every integer greater than 11 can be expressed as the sum of two composite numbers.
25. (a) Prove that all odd prime numbers can be expressed as the difference of squares of two successive integers.
    (b) Prove that no prime number can be expressed as the difference of two fourth powers of integers. (*Hint*: Use the factorization tool discussed in the final paragraph of this section.)
26. Prove or disprove the following statements.
    (a) If p is a prime number, then $2^p - 1$ is a prime number.
    (b) If $2^p - 1$ is a prime number, then p is a prime number. (*Hint*: Consider the contrapositive of the statement.)
27. Let a and n be positive integers with $n \neq 1$. Prove that, if $a^n - 1$ is a prime number, then $a = 2$ and n is a prime number. Conclude that the only prime numbers of the form $a^n - 1$ with $n \neq 1$ are Mersenne primes.
28. Let a and n be positive integers with $a > 1$. Prove that, if $a^n + 1$ is a prime number, then a is even and n is a power of 2.
29. Let n be a positive integer with $n \neq 1$. Prove that, if $n^2 + 1$ is a prime number, then $n^2 + 1$ is expressible in the form $4k + 1$ with $k \in \mathbf{Z}$.
30. Prove or disprove the following conjecture, which is similar to Conjecture 5.
    Conjecture: There are infinitely many prime numbers expressible in the form $n^3 + 1$ where n is a positive integer.
31. Prove or disprove the following conjecture.
    Conjecture: If n is a positive integer, then $n^2 - n + 41$ is a prime number.

1.3

Greatest Common Divisors

Given two integers a and b, not both zero, consider the set S of integers that divide both a and b. The set S is necessarily nonempty (since $\pm 1 \in S$) and finite (since zero is the only integer that has an infinite number of divisors and at least one of a and b is nonzero). So it makes sense to speak of the greatest element of S. Note that such an element is necessarily positive.

Definition 9: Let $a, b \in \mathbf{Z}$ with a and b not both zero. The ***greatest common divisor*** of a and b, denoted (a, b), is the greatest positive integer d such that $d \mid a$ and $d \mid b$. If $(a, b) = 1$, then a and b are said to be ***relatively prime.***

Note that $(0,0)$ is undefined. (Why?) Furthermore, it is easy to see that if $(a, b) = d$, then

$$(-a, b) = (a, -b) = (-a, -b) = d$$

So, in Example 11, we restrict our discussion to the computation of the greatest common divisor of two nonnegative integers.

Example 11:

(a) The divisors of 24 are ±1, ±2, ±3, ±4, ±6, ±8, ±12, and ±24. The divisors of 60 are ±1, ±2, ±3, ±4, ±5, ±6, ±10, ±12, ±15, ±20, ±30, and ±60. The common divisors of 24 and 60 are ±1, ±2, ±3, ±4, ±6, and ±12. So the greatest common divisor of 24 and 60 is 12, which is denoted $(24, 60) = 12$.

(b) Every integer is a divisor of zero. So the common divisors of 24 and 0 are precisely the divisors of 24; from (a) above, the greatest common divisor of 24 and 0 is 24, which is denoted $(24, 0) = 24$. In general, if $a \in \mathbf{Z}$ with $a \neq 0$, we have $(a, 0) = |a|$.

(c) The divisors of 35 are ±1, ±5, ±7, and ±35. From (a) above, the common divisors of 24 and 35 are ±1. So the greatest common divisor of 24 and 35 is 1, which is denoted $(24, 35) = 1$. In other words, 24 and 35 are relatively prime.

One crucial fact to remember when solving theoretical problems involving greatest common divisors is that $(a, b) = d$ implies $d \mid a$ and $d \mid b$; this observation in conjunction with Definition 1 or Proposition 1.2 or both is an extremely effective theoretical tool. At this point, it may be particularly instructive to attempt the solution of Exercises 36 and 38 with the above facts in mind.

We now prove two properties of greatest common divisors, which are recorded as propositions.

Proposition 1.10: Let $a, b \in \mathbf{Z}$ with $(a, b) = d$. Then $(a/d, b/d) = 1$.

Proof: Let $(a/d, b/d) = d'$. Then $d' \mid a/d$ and $d' \mid b/d$ so there exist $e, f \in \mathbf{Z}$ such that $a/d = d'e$ and $b/d = d'f$. So $a = d'de$ and $b = d'df$; consequently, we have $d'd \mid a$ and $d'd \mid b$. This implies that $d'd$ is a common divisor of a and b and, since d is the greatest common divisor of a and b, we have $d' = 1$, from which comes the desired result. ■

Proposition 1.11: Let $a, b \in \mathbf{Z}$ with a and b not both zero. Then

$$(a, b) = \min\{ma + nb \colon m, n \in \mathbf{Z}, ma + nb > 0\}$$

The set-theoretic function "min" produces the minimum element of a set. (Similarly, the set-theoretic function "max," to be used later, produces the maximum element of a set.) So Proposition 1.11 says that the greatest common divisor of two integers is the least positive number that is expressible as an integral linear combination of the integers.

Proof: (of Proposition 1.11) Note that $\{ma + nb : m, n \in \mathbf{Z}, ma + nb > 0\} \neq \varnothing$ since, without loss of generality, $a \neq 0$ and then either $1a + 0b > 0$ or $-1a + 0b > 0$. So $\min\{ma + nb : m, n \in \mathbf{Z},\ ma + nb > 0\}$ exists by the well-ordering property; let

$$d = \min\{ma + nb : m, n \in \mathbf{Z}, ma + nb > 0\} = m'a + n'b$$

We first show that $d \mid a$ and $d \mid b$. By the division algorithm, there exist $q, r \in \mathbf{Z}$ such that

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

Now

$$r = a - dq = a - (m'a + n'b)q = (1 - qm')a - qn'b$$

and we have that r is an integral linear combination of a and b. Since $0 \leq r < d$ and d is the minimum positive integral linear combination of a and b, we have $r = 0$, from which $a = dq + r$ implies that $a = dq$. So $d \mid a$. Similarly, $d \mid b$. It remains to show that d is the *greatest* common divisor of a and b. Let c be any common divisor of a and b so that $c \mid a$ and $c \mid b$. Then $c \mid m'a + n'b = d$ by Proposition 1.2, from which $c \leq d$. ■

Proposition 1.11 above gives another important theoretical tool when dealing with greatest common divisors, namely, that $(a, b) = d$ implies that d may be expressed as an integral linear combination of a and b. In fact, the converse of this fact is true if $d = 1$, namely, that if 1 is expressible as an integral linear combination of two integers a and b, then $(a, b) = 1$. (Why is this true?) We will use the tool of expressing the greatest common divisor of two integers as an integral linear combination of these integers in forthcoming chapters. Note further that Proposition 1.11 may be used to show that a common divisor of two integers is not only less than the greatest common divisor but also *divides* the greatest common divisor. (Do this!) This fact is also frequently useful in establishing theoretical results.

The concept of greatest common divisor can be extended to more than two integers.

Definition 10: Let $a_1, a_2, \ldots, a_n \in \mathbf{Z}$ with $a_1, a_2, \ldots, a_n$ not all zero. The *greatest common divisor* of $a_1, a_2, \ldots, a_n$, denoted $(a_1, a_2, \ldots, a_n)$, is the greatest integer d such that $d \mid a_i$, $i = 1, 2, \ldots, n$. If $(a_1, a_2, \ldots, a_n) = 1$, then $a_1, a_2, \ldots, a_n$ are said to be *relatively prime*. If $(a_i, a_j) = 1$ for all pairs i, j with $i \neq j$, then $a_1, a_2, \ldots, a_n$ are said to be *pairwise relatively prime.*

Example 12:

The divisors of 24 are ±1, ±2, ±3, ±4, ±6, ±8, ±12, and ±24. The divisors of 60 are ±1, ±2, ±3, ±4, ±5, ±6, ±10, ±12, ±15, ±20, ±30, and ±60. The divisors of 30 are ±1, ±2, ±3, ±5, ±6, ±10, ±15, and ±30. The common divisors of 24, 60, and 30 are ±1, ±2, ±3, and ±6. So the greatest common divisor of 24, 60, and 30 is 6, which is denoted $(24, 60, 30) = 6$. An alternate method for computing the greatest common divisor of more than two integers is investigated in Exercise 51.

Pairwise relatively prime integers are relatively prime; it is *not* the case that relatively prime integers are necessarily pairwise relatively prime as Example 13 illustrates.

Example 13:

Since $(24, 60, 49) = 1$ (verify this!), we have that 24, 60, and 49 are relatively prime. Since $(24, 60) = 12 \neq 1$ by Example 11(a), we have that 24, 60, and 49 are *not* pairwise relatively prime.

Exercise Set 1.3

32. Find the greatest common divisors below.
(a) $(21, 28)$
(b) $(32, 56)$
(c) $(58, 63)$
(d) $(0, 113)$
(e) $(111, 129)$
(f) $(120, 165)$

33. Let $a \in \mathbf{Z}$ with $a > 0$. Find the greatest common divisors below.
(a) (a, a^n) where n is a positive integer
(b) $(a, a + 1)$
(c) $(a, a + 2)$
(d) $(3a + 5, 7a + 12)$

34. Find the greatest common divisors below.
(a) $(18, 36, 63)$
(b) $(30, 42, 70)$
(c) $(0, 51, 0)$
(d) $(35, 55, 77)$
(e) $(36, 42, 54, 78)$
(f) $(35, 63, 70, 98)$

35. Find four integers that are relatively prime (when taken together) but such that no two of the integers are relatively prime when taken separately.

36. *(a)* Do there exist integers x and y such that $x + y = 100$ and $(x, y) = 8$? Why or why not?
(b) Prove that there exist infinitely many pairs of integers x and y such that $x + y = 87$ and $(x, y) = 3$.

37. Let $a, b \in \mathbf{Z}$ with a and b not both zero and let c be a nonzero integer. Prove that $(ca, cb) = |c|(a, b)$.

38. Let a and b be relatively prime integers. Prove that $(a + b, a - b)$ is either 1 or 2.

39. Let a and b be relatively prime integers. Find all values of $(a + 2b, 2a + b)$.

40. Let $a, b \in \mathbf{Z}$ with $(a, 4) = 2$ and $(b, 4) = 2$. Find $(a + b, 4)$ and prove that your answer is correct.

41. Let $a, b, c \in \mathbf{Z}$ with $(a, b) = 1$ and $c \mid a + b$. Prove that $(a, c) = 1$ and $(b, c) = 1$.

42. *(a)* Let $a, b, c \in \mathbf{Z}$ with $(a, b) = (a, c) = 1$. Prove that $(a, bc) = 1$.

(*b*) Let $a, b_1, b_2, \ldots, b_n \in \mathbf{Z}$ with $(a, b_1) = (a, b_2) = \cdots = (a, b_n) = 1$. Prove that

$$(a, b_1 b_2 \cdots b_n) = 1$$

43. (*a*) Let $a, b, c \in \mathbf{Z}$ with $(a, b) = 1$. Prove that if $a \mid c$ and $b \mid c$, then $ab \mid c$.
(*b*) Provide a counterexample to show why the statement of part (a) does not hold if $(a, b) \neq 1$.
(*c*) Let $a, a_2, \ldots, a_n$, $c \in \mathbf{Z}$ with $a_1, a_2, \ldots, a_n$ pairwise relatively prime. Prove that if $a_i \mid c$ for each i, then $a_1 a_2 \cdots a_n \mid c$.

44. (*a*) Let $a, b, c \in \mathbf{Z}$ with $(a, b) = 1$ and $a \mid bc$. Prove that $a \mid c$.
(*b*) Provide a counterexample to show why the statement of part (a) does not hold if $(a, b) \neq 1$.

45. Let a, b, c, and d be positive integers. If $b \neq d$ and $(a, b) = (c, d) = 1$, prove that $\frac{a}{b} + \frac{c}{d} \notin \mathbf{Z}$.

46. Let a, b, c, and d be integers with b and d positive and $(a, b) = (c, d) = 1$. A mistake often made when first encountering fractions is to assume that $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$. Find all solutions of this equation.

47. (*a*) Let $a, b \in \mathbf{Z}$ and let m be a nonnegative integer. Prove that $(a, b) = 1$ if and only if $(a^m, b) = 1$.
(*b*) Let $a, b \in \mathbf{Z}$ and let m and n be nonnegative integers. Prove that $(a, b) = 1$ if and only if $(a^m, b^n) = 1$.

48. Let $a, b \in \mathbf{Z}$. Prove that $(a, b) = 1$ if and only if $(a + b, ab) = 1$.

49. Prove that in any eight composite positive integers not exceeding 360, at least two are not relatively prime.

50. Prove that every integer greater than 6 can be expressed as the sum of two relatively prime integers greater than 1.

51. Let $a_1, a_2, \ldots, a_n \in \mathbf{Z}$ with $a_1 \neq 0$. Prove that

$$(a_1, a_2, a_3, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n)$$

(This method can be used generally to compute the greatest common divisor of more than two integers.) Use this method to compute the greatest common divisor of each set of integers in Exercise 34.

52. Let $a_1, a_2, \ldots, a_n \in \mathbf{Z}$ with $a_1 \neq 0$ and let c be a nonzero integer. Prove that

$$(ca_1, ca_2, ca_3, \ldots, ca_n) = |c|\,(a_1, a_2, a_3, \ldots, a_n).$$

53. Let $n \in \mathbf{Z}$. Prove that the integers $6n - 1$, $6n + 1$, $6n + 2$, $6n + 3$, and $6n + 5$ are pairwise relatively prime.

1.4

The Euclidean Algorithm

Our current method for finding the greatest common divisor of two integers is to list all divisors of each integer, find those divisors common to the two lists, and then choose the greatest such common divisor. Surely this method becomes unwieldy for large integers! (For example, what is the greatest common divisor of 803 and 154?) Is there a better method for computing the greatest common divisor of two integers? Yes, fortunately. Before discussing this method, we need a preliminary lemma.

Lemma 1.12: If $a, b \in \mathbf{Z}$, $a \geq b > 0$, and $a = bq + r$ with $q, r \in \mathbf{Z}$, then $(a, b) = (b, r)$.

Proof: Let c be a common divisor of a and b. Then $c \mid a$ and $c \mid b$ imply $c \mid a - qb$ by Proposition 1.2, from which $c \mid r$; we then have that c is a common divisor of b and r. Now let c be a common divisor of b and r so that $c \mid b$ and $c \mid r$. Then $c \mid qb + r$ by Proposition 1.2, from which $c \mid a$; we then have that c is a common divisor of a and b. So the common divisors of a and b are the same as the common divisors of b and r from which $(a, b) = (b, r)$. ■

The suggested method for computing the greatest common divisor of two positive integers is called the Euclidean algorithm after Euclid, who describes the algorithm in Book VII of his *Elements.* The Euclidean algorithm repeatedly uses the division algorithm (Theorem 1.4) to generate quotients and remainders from smaller and smaller pairs of positive integers. Eventually in this process, a remainder of zero is encountered, which terminates the algorithm; the greatest common divisor of the two integers is the remainder encountered just prior to the zero remainder. All of this is contained in the following theorem. As you read the theorem, note that the only parts requiring proof are the last three statements.

Theorem 1.13: (The Euclidean Algorithm) Let $a, b \in \mathbf{Z}$ with $a \geq b > 0$. By the division algorithm, there exist $q_1, r_1 \in \mathbf{Z}$ such that

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b$$

If $r_1 > 0$, there exist (by the division algorithm) $q_2, r_2 \in \mathbf{Z}$ such that

$$b = r_1 q_2 + r_2, \qquad 0 \leq r_2 < r_1$$

If $r_2 > 0$, there exist (by the division algorithm) $q_3, r_3 \in \mathbf{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \qquad 0 \leq r_3 < r_2$$

Continue this process. Then $r_n = 0$ for some n. If $n > 1$, then $(a, b) = r_{n-1}$. If $n = 1$, then $(a, b) = b$.

Proof: Note that $r_1 > r_2 > r_3 > \ldots$. If $r_n \neq 0$ for all n, then $r_1, r_2, r_3, \ldots$ is an infinite, strictly decreasing sequence of positive integers, which is impossible. So $r_n = 0$ for some n. Now, if $n > 1$, repeated applications of Lemma 1.12 give

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = (r_{n-1}, 0) = r_{n-1}$$

as desired. If $n = 1$, the desired statement is obvious. ■

Note that the Euclidean algorithm finds the greatest common divisor in the case of two *positive* integers, a and b (with $a \geq b$). In view of the remarks immediately after Definition 9 and the general remark in (b) of Example 11, all other computations are either reducible to this case or trivial. We now illustrate the use of the Euclidean algorithm with an example.

Example 14:

Find (803, 154) by using the Euclidean algorithm.
The notation of Theorem 1.13 is used throughout. Here $a = 803$ and $b = 154$. By the division algorithm,

$$803 = 154 \cdot 5 + 33 \tag{2}$$

Since $r_1 = 33 > 0$ apply the division algorithm to $b = 154$ and $r_1 = 33$ to obtain

$$154 = 33 \cdot 4 + 22 \tag{3}$$

Since $r_2 = 22 > 0$, apply the division algorithm to $r_1 = 33$ and $r_2 = 22$ to obtain

$$33 = 22 \cdot 1 + 11 \tag{4}$$

Since $r_3 = 11 > 0$, we apply the division algorithm to $r_2 = 22$ and $r_3 = 11$ to obtain

$$22 = 11 \cdot 2 + 0$$

Since $r_4 = 0$, the Euclidean algorithm terminates and

$$(803, 154) = r_3 = 11$$

Recall that, by Proposition 1.11, the greatest common divisor of two integers is expressible as an integral linear combination of the two integers. (As already noted, this expression will be used in forthcoming chapters.) The Euclidean algorithm provides a systematic procedure for obtaining such a linear combination, as the following example illustrates.

Example 15:

Express (803, 154) as an integral linear combination of 803 and 154.
Essentially, work through the steps of Example 14 backward. We have

$$\begin{aligned}(803, 154) = 11 &= 33 - 22 \quad [\text{by } (4)]\\ &= 33 - (154 - 33 \cdot 4) \quad [\text{by } (3)]\\ &= 33 \cdot 5 - 154\\ &= (803 - 154 \cdot 5)5 - 154 \quad [\text{by } (2)]\\ &= 803 \cdot 5 - 154 \cdot 26\\ &= 5 \cdot 803 + (-26)154\end{aligned}$$

This is an expression of (803, 154) as an integral linear combination of 803 and 154 as desired. Two remarks are in order here. First, by Proposition 1.11, the greatest common divisor of two integers is the least positive number expressible as an integral linear combination of the integers. So *no* integral linear combination of 803 and 154 can yield any of the integers $10, 9, \dots, 1$. Second, the expression of 11 as an integral linear combination of 803 and 154 above is *not* unique. For example, the reader may verify that $11 = 19\cdot 803 - 99\cdot 154$ is another such expression. In fact, there are infinitely many expressions of 11 as an integral linear combination of 803 and 154. We will have more to say on this issue in Chapter 6.

A useful programming project related to Examples 14 and 15 appears as Student Project 1.

Exercise Set 1.4

54. Use the Euclidean algorithm (Theorem 1.13) to find the greatest common divisors below. Express each greatest common divisor as an integral linear combination of the original integers.
    (a) $(37, 60)$
    (b) $(78, 708)$
    (c) $(441, 1155)$
    (d) $(793, 3172)$
    (e) $(2059, 2581)$
    (f) $(25174, 42722)$
55. Prove that 7 has no expression as an integral linear combination of 18209 and 19043.
56. Find two rational numbers with denominators 11 and 13, respectively, and a sum of $\frac{7}{143}$.
57. Use Exercise 51 and the Euclidean algorithm to find the greatest common divisors below. Express each greatest common divisor as an integral linear combination of the original integers.
    (a) $(221, 247, 323)$
    (b) $(210, 294, 490, 735)$
58. [The following exercise presents an algorithm for computing the greatest common divisor of two positive integers analogous to the Euclidean algorithm. This new algorithm is based on the absolute least remainder algorithm given in part (c) of Exercise 15.] Let $a, b \in \mathbf{Z}$ with $a \geq b > 0$. By the absolute least remainder algorithm, there exist $q_1, r_1 \in \mathbf{Z}$ such that

$$a = bq_1 + r_1, \qquad -\frac{|b|}{2} < r_1 \leq \frac{|b|}{2}$$

If $r_1 \neq 0$, there exist (by the absolute least remainder algorithm) $q_2, r_2 \in \mathbf{Z}$ such that

$$b = r_1q_2 + r_2, \qquad -\frac{|r_1|}{2} < r_2 \leq \frac{|r_1|}{2}$$

If $r_2 \neq 0$, there exist (by the absolute least remainder algorithm) $q_3, r_3 \in \mathbf{Z}$ such that

$$r_1 = r_2q_3 + r_3, \qquad -\frac{|r_2|}{2} < r_3 \leq \frac{|r_2|}{2}$$

Continue this process.

(a) Prove that $r_n = 0$ for some n. If $n > 1$, prove that $(a, b) = |r_{n-1}|$.

(b) Use the new algorithm above to find $(204, 228)$ and $(233, 377)$.

1.5

The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic (the essence of which appears as Proposition 14 in Book IX of Euclid's *Elements*) is our first big theorem of number theory, but certainly not our last! This theorem guarantees that any integer greater than 1 can be decomposed into a product of prime numbers; furthermore, this decomposition is unique except for the order in which the prime numbers are listed. (For example, the decomposition of 12 into $2 \cdot 2 \cdot 3$ is the same as the decomposition of 12 into $2 \cdot 3 \cdot 2$ except for the order in which the two 2's and one 3 are listed.) We first prove an important preliminary lemma.

Lemma 1.14: (Euclid) Let $a, b, p \in \mathbf{Z}$ with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Assume that $p \nmid a$. Then $(a, p) = 1$. We must show that $p \mid b$. By Proposition 1.11, there exist $m, n \in \mathbf{Z}$ such that $ma + np = 1$. Also, $p \mid ab$ implies $ab = pc$ for some $c \in \mathbf{Z}$. Now multiplying both sides of $ma + np = 1$ by b, we have $mab + npb = b$; $ab = pc$ then implies that $mpc + npb = b$ or $p(mc + nb) = b$. So we have $p \mid b$ as desired. ■

Note that Lemma 1.14 does not hold if p is composite. (Your solution to Exercise 2 in Section 1 should provide a counterexample.) In view of this, the criterion in Lemma 1.14 could be used to *define* a prime number as follows:

> An integer $p > 1$ is said to be *prime* if whenever a and b are integers with $p \mid ab$, then $p \mid a$ or $p \mid b$.

This alternate definition of *prime* is useful in more general mathematical settings (see, for example, Definition 3.3 on page 136 of Hungerford, 1974); in the system of integers, we have opted instead for the more traditional definition given in Definition 5.

Lemma 1.14 above can be generalized. We state this generalization as a corollary in which we use the powerful proof technique called *mathematical induction*. Mathematical induction will be used frequently in this book, especially in Chapter 7. (You may have already used mathematical induction a few times in the preceding exercises.) See Appendix A for a discussion of mathematical induction.

Corollary 1.15: Let $a_1, a_2, \ldots, a_n, p \in \mathbf{Z}$ with p prime. If $p \mid a_1a_2 \cdots a_n$, then $p \mid a_i$ for some i.

Proof: We use induction on n. The statement for $n = 1$ is obvious. The statement for $n = 2$ is Lemma 1.14. Assume that $k \geq 2$ and that the desired statement is true for $n = k$ so that $p \mid a_1a_2 \cdots a_k$ implies that $p \mid a_i$ for some i (with $1 \leq i \leq k$). We must show that $p \mid a_1a_2 \cdots a_{k+1}$ implies that $p \mid a_i$ for some i (with $1 \leq i \leq k + 1$) so that the desired statement holds for $n = k + 1$. Now $p \mid a_1 a_2 \cdots a_{k+1}$ implies $p \mid (a_1 a_2 \cdots a_k)a_{k+1}$; Lemma 1.14 then implies $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$. If $p \mid a_{k+1}$, then the desired statement holds for $n = k + 1$. If $p \nmid a_{k+1}$, then $p \mid a_1 a_2 \cdots a_k$, which implies that $p \mid a_i$ for some i (with $1 \leq i \leq k$) by the induction hypothesis, and the desired statement holds for $n = k + 1$, which completes the proof. ■

We now state and prove the Fundamental Theorem of Arithmetic.

Theorem 1.16: (Fundamental Theorem of Arithmetic) Every integer greater than 1 can be expressed in the form $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ with $p_1, p_2, \ldots, p_n$ distinct prime numbers and $a_1, a_2, \ldots, a_n$ positive integers. This form is said to be the *prime factorization* of the integer. This prime factorization is unique except for the arrangement of the $p_i^{a_i}$.

Proof: Assume, by way of contradiction, that k is an integer greater than 1 that does not have an expression as in the statement of the theorem. Without loss of generality, we may assume that k is the least such integer. Now k cannot be prime because it would then be of the desired form. So k is composite and $k = ab$ with $1 < a < k$ and $1 < b < k$. But then a and b are of the desired form due to the minimality of k, from which it follows that k is of the desired form, a contradiction. So every integer greater than 1 has an expression of the desired form. We still must show the uniqueness of such an expression. Assume that k has two such expressions, say

$$k = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$$

with $p_1, p_2, \ldots, p_n$ distinct prime numbers; $q_1, q_2, \ldots, q_m$ distinct prime numbers; and $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_m$ positive integers. Without loss of generality, we may assume that $p_1 < p_2 < \cdots < p_n$ and $q_1 < q_2 < \cdots < q_m$. We must show that

$$n = m$$

$$p_i = q_i, \quad i = 1, 2, \ldots, n$$

and

$$a_i = b_i, \quad i = 1, 2, \ldots, n$$

Now, given a p_i, we have $p_i \mid q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$, which implies that $p_i \mid q_j$ for some j by Corollary 1.15. So $p_i = q_j$ for some j. Similarly, given a q_j, we have $q_j = p_i$ for some i. So $n = m$; by the ordering of the p_i's and q_j's, we have $p_i = q_i$, $i = 1, 2, \ldots, n$. Consequently,

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

Now assume, by way of contradiction, that $a_i \neq b_i$ for some i. Without loss of generality, we may assume that $a_i < b_i$. Then

$$p_i^{b_i} \mid p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

which implies that

$$p_i^{b_i - a_i} \mid p_1^{a_1} p_2^{a_2} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}$$

Since $b_i - a_i > 0$, we have that

$$p_i \mid p_1^{a_1} p_2^{a_2} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}$$

from which $p_i \mid p_j$ for some $j \neq i$, by Corollary 1.15. This is a contradiction. So $a_i = b_i$, $i = 1, 2, \ldots, n$. ■

Example 16:

Find the prime factorization of 756.

We have

$$\begin{aligned} 756 &= 2 \cdot 378 \\ &= 2 \cdot 2 \cdot 189 \\ &= 2 \cdot 2 \cdot 3 \cdot 63 \\ &= 2 \cdot 2 \cdot 3 \cdot 7 \cdot 9 \\ &= 2 \cdot 2 \cdot 3 \cdot 7 \cdot 3 \cdot 3 \\ &= 2^2 3^3 7 \end{aligned}$$

Because of our familiarity with the integers, we may tend to take the Fundamental Theorem of Arithmetic for granted. Note, however, that number systems exist for which unique factorization does *not* hold. Such a system is investigated more fully in Exercise 77. The presence of the Fundamental Theorem of Arithmetic for the integers makes the integers into what is called a *unique factorization domain* (*UFD*). UFDs are important number systems in a more advanced branch of number theory called *algebraic number theory.* The moral here is to appreciate the Fundamental Theorem of Arithmetic for the extremely nice property that it is!

A concept that is parallel to the greatest common divisor of two integers is the least common multiple of the integers, which we define now.

Definition 11: Let $a, b \in \mathbf{Z}$ with $a, b > 0$. The *least common multiple* of a and b, denoted $[a, b]$, is the least positive integer m such that $a \mid m$ and $b \mid m$.

Given two positive integers a and b, note that $ab > 0$, $a \mid ab$, and $b \mid ab$; in other words, ab is always a positive common multiple of a and b. Hence the set of positive common multiples of two positive integers is always nonempty; consequently, the *least* common multiple of these integers always exists by the well-ordering property of the integers (see the Introduction).

Example 17:

(a) The positive multiples of 6 are $6, 12, 18, 24, 30, 36, 42, 48, \ldots$. The positive multiples of 7 are 7, 14, 21, 28, 35, 42, 49, 54, ... It is a fact (perhaps not obvious) that the positive *common* multiples of 6 and 7 (the multiples common to the two infinite lists above) are $42, 84, 126, 168, 210, \ldots$. (Convince yourself of this!) Obviously from these common multiples of 6 and 7, the least common multiple of 6 and 7 is 42, which is denoted $[6, 7] = 42$.

(b) The positive multiples of 8 are $8, 16, 24, 32, 40, 48, 56, 64, \ldots$. From the multiples of 6 in (a) above, it is obvious that the least common multiple of 6

and 8 is 24, which is denoted $[6,8] = 24$. (As an exercise, find the first five positive common multiples of 6 and 8.)

The Fundamental Theorem of Arithmetic may be used to compute greatest common divisors and least common multiples. We illustrate such computations with an example.

Example 18:

Find $(756, 2205)$ and $[756, 2205]$ by using prime factorization.

By Example 16, we have $756 = 2^2 3^3 7$. The reader may easily verify that $2205 = 3^2 5 \cdot 7^2$. Now

$$756 = 2^2 3^3 5^0 7^1$$

and

$$2205 = 2^0 3^2 5^1 7^2$$

For $(756, 2205)$, we compare the exponents appearing on like prime numbers and choose the minimum exponent appearing in each comparison [since $(756, 2205)$ must divide both 756 and 2205]. So

$$(756, 2205) = 2^0 3^2 5^0 7 = 63$$

Similarly, for $[756, 2205]$, we compare the exponents appearing on like prime numbers and choose the maximum exponent appearing in each comparison (since both 756 and 2205 must divide $[756, 2205]$). So

$$[756, 2205] = 2^2 3^3 5^1 7^2 = 26460$$

Example 18 motivates the following proposition.

Proposition 1.17: Let $a, b \in \mathbf{Z}$ with $a, b > 1$. Write $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ where $p_1, p_2, \ldots, p_n$ are distinct prime numbers and $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ are nonnegative integers (possibly zero). Then

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

and

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

Proof: The proof is obvious from the Fundamental Theorem of Arithmetic (Theorem 1.16) and the definitions of (a, b) and $[a, b]$. ■

It is instructive to pause here. Proposition 1.17 seemingly gives us a beautiful way to compute greatest common divisors and least common multiples of positive integers. Has our Euclidean algorithm (for computation of the greatest common divisor) been rendered obsolete? The answer is a resounding *no.* While Proposition 1.17 is useful as a theoretical result, it has little practical use except for computations involving greatest common divisors and least common multiples of relatively small integers. Proposition 1.17 requires the computation of prime factorizations. Unfortunately, prime factorizations of large integers are generally difficult to obtain. [The interested reader may wish to consult Bressoud (1990) in this regard.] The power inherent in the Euclidean algorithm is that greatest common divisors of integers may be computed *without obtaining the prime factorizations of the integers.* But what about least common multiples? Our goal here is to establish a simple relationship between the least common multiple and the greatest common divisor of two positive integers; the desired result is a practical method for computing least common multiples. We first need an easy lemma.

Lemma 1.18: Let $x, y \in \mathbf{R}$. Then $\max\{x, y\} + \min\{x, y\} = x + y$.

Proof: If $x < y$, then $\max\{x, y\} = y$ and $\min\{x, y\} = x$, and the desired result follows. The cases are similar for $x = y$ and $x > y$. ■

The relationship between the greatest common divisor and the least common multiple of two positive integers is now given by the following theorem.

Theorem 1.19: Let $a, b \in \mathbf{Z}$ with $a, b > 0$. Then $(a, b)[a, b] = ab$.

Proof: If $a, b > 1$, write $a = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ and $b = p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$ as in Proposition 1.17. Then

$$\begin{aligned}(a, b)[a, b] &= \{p_1^{\min\{a_1,b_1\}}p_2^{\min\{a_2,b_2\}}\cdots p_n^{\min\{a_n,b_n\}}\}\{p_1^{\max\{a_1,b_1\}}p_2^{\max\{a_2,b_2\}}\cdots p_n^{\max\{a_n,b_n\}}\}\\ &= p_1^{\min\{a_1,b_1\}+\max\{a_1,b_1\}}p_2^{\min\{a_2,b_2\}+\max\{a_2,b_2\}}\cdots p_n^{\min\{a_n,b_n\}+\max\{a_n,b_n\}}\\ &= p_1^{a_1+b_1}p_2^{a_2+b_2}\cdots p_n^{a_n+b_n} \quad \text{(by Lemma 1.18)}\\ &= p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}\\ &= ab\end{aligned}$$

as desired. The cases $a = 1$ and $b > 1$, $a > 1$ and $b = 1$, and $a = b = 1$ are easily checked and are left as exercises. ■

So, to find the least common multiple of two positive integers without using prime factorization, one finds the greatest common divisor of the two integers by using the Euclidean algorithm and then Theorem 1.19 to obtain the least common multiple. Again, this method is usually much easier than using Proposition 1.17, which requires the prime factorizations of the integers! The reader is invited to pause here to compute $[803, 154]$ using $(803, 154) = 11$ from Example 14.

Note in Example 17 that the least common multiple of 6 and 7 was the product of 6 and 7, while the least common multiple of 6 and 8 was *not* the product of 6 and 8. (Is the least common multiple of 803 and 154 the product of 803 and 154?) Under what circumstances is the least common multiple of two positive integers simply the product of the two integers? In view of Theorem 1.19, the answer is not surprising, as the next corollary shows.

Corollary 1.20: Let $a, b \in \mathbf{Z}$ with $a, b > 0$. Then $[a, b] = ab$ if and only if $(a, b) = 1$.

Proof: The (extremely easy) proof is left as an exercise for the reader. ■

We conclude this chapter with another illustration of the power of the

Biography

Peter Gustav Lejeune Dirichlet (1805–1859)

P. G. L. Dirichlet was a student of Gauss and Gauss's successor at Göttingen University. Born in Germany, Dirichlet was fluent in both German and French and served as a mathematical liasion between Germany and France. Along with his close friend Jacobi (see the latter's biography in Chapter 4), Dirichlet aided in the shift of mathematical activity from France to Germany in the nineteenth century. Dirichlet authored *Vorlesungen über Zahlentheorie,* a work essentially devoted to the further understanding of the many treasures in Gauss's profound *Disquisitiones Arithmeticae.* In addition, he analyzed the convergence of Fourier series and proved the theorem on prime numbers in arithmetic progressions below. Dirichlet frequently relied on the principles of real and complex analysis in his proofs; as such, Dirichlet set the stage for that area of mathematics known as *analytic number theory.*

Fundamental Theorem of Arithmetic. We begin by stating a famous theorem of number theory from P. G. L. Dirichlet. This theorem generalizes Euclid's theorem on the infinitude of the prime numbers (Theorem 1.6). Unfortunately, the proof of this theorem is beyond the scope of this book.

Theorem 1.21: (Dirichlet's Theorem on Prime Numbers in Arithmetic Progressions) Let $a, b \in \mathbf{Z}$ with $a, b > 0$ and $(a, b) = 1$. Then the arithmetic progression

$$a, a + b, a + 2b, \ldots, a + nb, \ldots$$

contains infinitely many prime numbers.

Note that Theorem 1.6 (the infinitude of the prime numbers) follows from

Theorem 1.21 above by putting $a = b = 1$. Dirichlet's Theorem, however, may be used to establish many other interesting facts, one of which is investigated in Exercise 84. The next proposition is a special case of Dirichlet's Theorem (with $a = 3$ and $b = 4$).

Proposition 1.22: There are infinitely many prime numbers expressible in the form $4n + 3$ where n is a nonnegative integer.

The Fundamental Theorem of Arithmetic allows us to prove the special case of Dirichlet's Theorem given in Proposition 1.22 above. We need a preliminary lemma.

Lemma 1.23: Let $a, b \in \mathbf{Z}$. If a and b are expressible in the form $4n + 1$ where n is an integer, then ab is also expressible in that form.

Proof: Let $a = 4n_1 + 1$ and $b = 4n_2 + 1$ with $n_1, n_2 \in \mathbf{Z}$. Then

$$\begin{aligned} ab &= (4n_1 + 1)(4n_2 + 1) = 16n_1n_2 + 4n_1 + 4n_2 + 1 \\ &= 4(4n_1n_2 + n_1 + n_2) + 1 \\ &= 4n + 1 \end{aligned}$$

where $n = 4n_1n_2 + n_1 + n_2 \in \mathbf{Z}$. ■

We now prove Proposition 1.22.

Proof: (of Proposition 1.22) Assume, by way of contradiction, that there are only finitely many prime numbers of the form $4n + 3$ where n is a nonnegative integer, say $p_0 = 3$, $p_1, p_2, \ldots, p_r$. (Here the prime numbers $p_1, p_2, \ldots, p_r$ are assumed to be distinct from 3.) Consider the number $N = 4p_1p_2 \cdots p_r + 3$. The prime factorization of N must contain a prime number p of the desired form or it would otherwise contain only prime numbers of the form $4n + 1$ where n is a positive integer (see Exercise 85) and hence be of the form $4n + 1$ where n is a positive integer by Lemma 1.23. So $p = p_0 = 3$ or $p = p_i$, $i = 1, 2, \ldots, r$.
Case I: $p = p_0 = 3$
Then $3 \mid N$ implies $3 \mid N - 3$ by Proposition 1.2, and we have that $3 \mid 4p_1p_2 \cdots p_r$. By Corollary 1.15, we now have $3 \mid 4$ or $3 \mid p_i$, $i = 1, 2, \ldots, r$, a contradiction.
Case II: $p = p_i$, $i = 1, 2, \ldots, r$
Then $p_i \mid N$ implies $p_i \mid N - 4p_1p_2 \cdots p_r$ by Proposition 1.2, and we have that $p_i \mid 3$, a contradiction.
So there are infinitely many prime numbers of the desired form. ■

Note the ingenuity in the construction of the number N above, because it is precisely consideration of this number that results in the desired contradictions. (Where have we seen such ingenuity before?) More important, Proposition 1.22 was billed as an application of the Fundamental Theorem of Arithmetic; where was the Fundamental Theorem of Arithmetic used in the proof of Proposition 1.22 above?

The proof of Proposition 1.22 cannot be extended to prove Dirichlet's Theorem in general, since the analogue of Lemma 1.23 is not true in general (see Exercise 86). The analogue of Lemma 1.23 is true in other special cases of Dirichlet's Theorem, one of which is investigated in Exercise 87.

Exercise Set 1.5

59. Find the prime factorization of each integer below.
(a) 51
(b) 87
(c) 361
(d) 367
(e) 422
(f) 945
(g) 1001
(h) 6292

60. Find the least common multiples below.
(a) [6,9]
(b) [7,9]
(c) [13,91]
(d) [24,60]
(e) [100,105]
(f) [101,1111]

61. Find the greatest common divisor and the least common multiple of each pair of integers below.
(a) $2^2 \cdot 3^3 \cdot 5 \cdot 7$, $2^2 \cdot 3^2 \cdot 5 \cdot 7^2$
(b) $2^2 \cdot 5^2 \cdot 7^3 \cdot 11^2$, $3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$
(c) $2^2 \cdot 5^7 \cdot 11^{13}$, $3^2 \cdot 7^5 \cdot 13^{11}$
(d) $3 \cdot 17 \cdot 19^2 \cdot 23$, $5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 29$

62. Find five integers that are relatively prime (when taken together) but such that no two of the integers are relatively prime when taken separately.

63. Find each of the least common multiples below by using the Euclidean algorithm and Theorem 1.19.
(a) [221,323]
(b) [257,419]
(c) [313,1252]
(d) [1911,9702]

64. Find all pairs of positive integers a and b such that $(a, b) = 12$ and $[a, b] = 360$.

65. ***Definition:*** Let $a_1, a_2, \dots, a_n \in \mathbf{Z}$ with $a_1, a_2, \dots, a_n$ nonzero. The *least common multiple* of $a_1, a_2, \dots, a_n$, denoted $[a_1, a_2, \dots, a_n]$, is the least positive integer m such that $a_i \mid m$, $i = 1, 2, \dots, n$.
Find the least common multiples below.

(a) $[10, 12, 15]$
(b) $[9, 13, 16]$
(c) $[6, 7, 8, 9]$

66. Why is 1 excluded as a prime number?

67. (a) Let $n \in \mathbf{Z}$ with $n > 1$. Prove that n is a perfect square if and only if all exponents in the prime factorization of n are even.
(b) Let $n \in \mathbf{Z}$ with $n > 0$. Prove that n is the product of a perfect square and (possibly zero) distinct prime numbers.

68. Let $n \in \mathbf{Z}$ with $n > 0$. Prove that there exist $k, m \in \mathbf{Z}$ with m odd such that $n = 2^k m$.

69. *Definition:* Let $n \in \mathbf{Z}$ with $n > 1$. Then n is said to be *powerful* if all exponents in the prime factorization of n are at least 2.
Prove that a powerful number is the product of a perfect square and a perfect cube.

70. Prove or disprove the following statements.
(a) If $a, b \in \mathbf{Z}$, $a, b > 0$, and $a^2 \mid b^3$, then $a \mid b$.
(b) If $a, b \in \mathbf{Z}$, $a, b > 0$, and $a^2 \mid b^2$, then $a \mid b$.
(c) If $a \in \mathbf{Z}$, $a > 0$, p is a prime number, and $p^4 \mid a^3$, then $p^2 \mid a$.

71. Let n, a, and b be positive integers such that $ab = n^2$. If $(a, b) = 1$, prove that there exist positive integers c and d such that $a = c^2$ and $b = d^2$.

72. *Definition:* Let n and a be positive integers and let p be a prime number. Then p^a is said to *exactly divide n*, denoted $p^a \parallel n$, if $p^a \mid n$ and $p^{a+1} \nmid n$.
Assume that $p^a \parallel m$ and $p^b \parallel n$.
(a) What power of p exactly divides $m + n$? Prove your assertion.
(b) What power of p exactly divides mn? Prove your assertion.
(c) What power of p exactly divides m^n? Prove your assertion.

73. Let $n \in \mathbf{Z}$ with $n > 0$. Find the largest integer guaranteed to divide *all* products of n consecutive integers and prove your assertion. (*Hint*: Consider several small values of n and look for a pattern.)

74. Find all positive integers a and b such that $a^b = b^a$.

75. (*Note*: You may wish to review Exercise 14 before attempting this problem.)
(a) Find the number of positive integers not exceeding 500 that are divisible by 2 and by 3.
(b) Find the number of positive integers not exceeding 500 that are divisible by neither 2 nor 3.
(c) Find the number of positive integers not exceeding 500 that are divisible by 2 but not by 3.

76. (a) Let $n \in \mathbf{Z}$ with $n > 1$, and let p be a prime number. If $p \mid n!$, prove that the exponent of p in the prime factorization of $n!$ is $[n/p] + [n/p^2] + [n/p^3] + \cdots$. (Note· that this sum is finite, since $[n/p^m] = 0$ if $p^m > n$.)
(b) Use part (a) above to find the prime factorization of 20!.
(c) Find the number of zeros with which the decimal representation of 100! terminates.

77. (The following exercise develops a number system that does not possess unique factorization and thus no Fundamental Theorem of Arithmetic.) Let $\mathbf{Z}[\sqrt{-10}]$ denote the set of all complex numbers of the form

$a + b\sqrt{-10}$ with $a, b \in \mathbf{Z}$ under the usual operations of addition and multiplication of complex numbers. Define an element $a + b\sqrt{-10}$ of $\mathbf{Z}[\sqrt{-10}]$ to be *irreducible* if $a + b\sqrt{-10}$ cannot be expressed as a product of two elements of $\mathbf{Z}[\sqrt{-10}]$ except as the trivial factorizations

$$a + b\sqrt{-10} = (1)(a + b\sqrt{-10})$$

or

$$a + b\sqrt{-10} = (-1)(-a - b\sqrt{-10})$$

(*a*) Prove that 2 and 7 are irreducible elements in $\mathbf{Z}[\sqrt{-10}]$.

(*b*) Prove that $2 + \sqrt{-10}$ and $2 - \sqrt{-10}$ are irreducible elements in $\mathbf{Z}[\sqrt{-10}]$. [*Hint*: For $2 + \sqrt{-10}$, assume that $2 + \sqrt{-10} = (a + b\sqrt{-10})(c + d\sqrt{-10})$ with $a, b, c, d \in \mathbf{Z}$. Then $2 - \sqrt{-10} = (a - b\sqrt{-10})(c - d\sqrt{-10})$ (why?). Now multiply the left-hand sides and the right-hand sides of the two equations and prove that the factorization of $2 + \sqrt{-10}$ must be a trivial factorization.]

(*c*) Prove that $\mathbf{Z}[\sqrt{-10}]$ does not possess unique factorization into irreducible elements. [*Hint*: In $\mathbf{Z}[\sqrt{-10}]$, we have $14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$.]

78. Let $n \in \mathbf{Z}$ with $n > 1$. Prove that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \notin \mathbf{Z}$.

79. Let a and b be positive integers.

(*a*) Prove that $(a, b) \mid [a, b]$.

(*b*) Find and prove a necessary and sufficient condition that $(a, b) = [a, b]$.

80. Let a, b, and c be positive integers. Prove that $[ca, cb] = c[a, b]$.

81. Let $a_1, a_2, \ldots, a_n$ be positive integers. Prove that

$$[a_1, a_2, a_3, \ldots, a_n] = [[a_1, a_2], a_3, \ldots, a_n].$$

(This method can be used generally to compute the least common multiple of more than two integers.) Use this method to compute the least common multiple of each set of integers in Exercise 65.

82. Let $a_1, a_2, \ldots, a_n$, and c be positive integers. Prove that

$$[ca_1, ca_2, ca_3, \ldots, ca_n] = c[a_1, a_2, a_3, \ldots, a_n].$$

83. Let $a, b \in \mathbf{Z}$ with $a, b > 0$ and $(a, b) = 1$. Prove that the arithmetic progression

$$a, a + b, a + 2b, \ldots, a + nb, \ldots$$

contains infinitely many composite numbers.

84. Let $k \in \mathbf{Z}$ with $k > 0$. Prove that there are infinitely many prime numbers ending in k 1's.

85. (*a*) Prove that any integer is expressible in the form $4n$, $4n + 1$, $4n + 2$, or $4n + 3$ where n is an integer.

(*b*) Prove that any odd number is expressible in the form $4n + 1$ or $4n + 3$ where n is an integer.

86. Prove that the analogue of Lemma 1.23 is not true for numbers of the form $4n + 3$ where n is an integer.

87. (*a*) Let $a, b \in \mathbf{Z}$. Prove that if a and b are expressible in the form $6n + 1$, where n is an integer, then ab is also expressible in that form.

(*b*) Prove that there are infinitely many prime numbers of the form $6n + 5$

where n is an integer. (*Hint*: Assume, by way of contradiction, that there are only finitely many prime numbers of the desired form and ingeniously construct a number N that will eventually lead to a contradiction. In other words, parallel the proof of Proposition 1.22.)

1.6 Concluding Remarks

The importance of divisibility and factorization in elementary number theory cannot be overestimated; the concepts and ideas presented in this chapter will appear again and again in succeeding chapters. The repercussions of the Fundamental Theorem of Arithmetic will be monumental. (Moral: Learn these concepts and ideas *now*!) The ultimate simplicity of these concepts has its disadvantages: Many of the open problems in elementary number theory are easily stated but maddeningly difficult to prove. (Go back and look at the conjectures in this chapter. How many of these conjectures would you have guessed still require proofs or counterexamples?) The simple nature of elementary number theory seemingly does not give us adequate techniques for attacking these questions; most mathematicians focus on more advanced algebraic and analytic techniques in their attempts to find solutions to these problems. It is perhaps unexpected (but certainly fascinating!) that the integers apparently contain so many secrets waiting to be discovered.

Student Projects

1. (Programming project for calculator or computer)
   (a) Given positive integers a and b, compute (a, b) by using the Euclidean algorithm.
   (b) Given positive integers a and b, express (a, b) as an integral linear combination of a and b.
2. Prove or disprove the following conjectures.
   Conjecture: If n is a nonnegative integer, then $n^2 - 79n + 1601$ is a prime number.
   Conjecture: If n is a nonnegative integer, then $n^2 + n + 41$ is a prime number.
   [A discussion of prime-producing polynomials of the form $n^2 + n + c$ (as in the second conjecture above) may be found in Daniel Fendel, "Prime-producing Polynomials and Principal Ideal Domains," *Mathematics Magazine, 58* (1985), 204–210.]
3. *(a)* Let p_n denote the nth prime number. Prove that the infinite series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges. (A short proof of this fact can be found in Apostol, 1976).
   (b) Do some research to find the behavior of the series $\sum_{p} \frac{1}{p}$, where p ranges over all twin primes.

4. Two integers m and n between 2 and 100 inclusive are chosen. The sum of the two integers is given to one mathematician, Sam, and the product of the two integers is given to another mathematician, Prudence. Suppose that, after some thought, the two mathematicians exchange the following dialogue:

   Prudence: "I don't know your sum, Sam."
   Sam: "I knew that you didn't, Prudence."
   Prudence: "Now I know your sum."
   Sam: "And now I know your product."

   What are m and n?

   [A discussion of the problem above and similar problems may be found in John O. Kiltinen & Peter B. Young, "Goldbach, Lemoine, and a Know/Don't Know Problem," *Mathematics Magazine, 58* (1985), 195–203.]

5. Answer the problem posed by Archimedes Andrews at the conclusion of the following article: Barry A. Cipra, "Archimedes Andrews and the Euclidean Time Bomb," *Mathematical Intelligencer, 9* (1987), 44–47.

6. For positive integral n, consider the function

$$h(n) = \begin{cases} \dfrac{n}{2}, & \textit{if } n \text{ is even} \\ 3n + 1, & \text{if } n \text{ is odd} \end{cases}$$

   Given n, one may iterate the function $h(n)$ to obtain a sequence of positive integers $\{n, h(n), h(h(n)), h(h(h(n))), \ldots\}$. For example, the sequence associated with the starting integer 6 is $\{6, 3, 10, 5, 16, 8, 4, 2, 1, \ldots\}$. By experimenting with various starting values of n, formulate a conjecture concerning the behavior of the associated sequences.

   [There is a famous unsolved problem concerning the function $h(n)$ that you may have formulated above as a conjecture. For further discussion of this problem, consult section 11.3 of the following book: Clifford A. Pickover, *Computers, Pattern, Chaos and Beauty* (New York: St. Martin's Press, 1990).]

7. Find the next term in the following sequence:

$$2, \quad 12, \quad 360, \quad 75600, \quad 174636000, \quad \ldots$$

   [This sequence, created by Paul Chernoff, is discussed in Chapter 66 of the following book: Clifford A. Pickover, *Mazes for the Mind: Computers and the Unexpected* (New York: St. Martin's Press, 1992).]