CHAPTER 2

DIVISIBILITY THEORY IN THE INTEGERS

Integral numbers are the fountainhead of all mathematics.
H. Minkowski

2.1 EARLY NUMBER THEORY

Before becoming weighted down with detail, we should say a few words about the origin of number theory. The theory of numbers is one of the oldest branches of mathematics; an enthusiast, by stretching a point here and there, could extend its roots back to a surprisingly remote date. Although it seems probable that the Greeks were largely indebted to the Babylonians and ancient Egyptians for a core of information about the properties of the natural numbers, the first rudiments of an actual theory are generally credited to Pythagoras and his disciples.

Our knowledge of the life of Pythagoras is scanty, and little can be said with any certainty. According to the best estimates, he was born between 580 and 562 B.C. on the Aegean island of Samos. It seems that he studied not only in Egypt, but may even have extended his journeys as far east as Babylonia. When Pythagoras reappeared after years of wandering, he sought out a favorable place for a school and finally settled upon Croton, a prosperous Greek settlement on the heel of the Italian boot. The school concentrated on four *mathemata*, or subjects of study: *arithmetica* (arithmetic, in the sense of number theory, rather than the art of calculating), *harmonia* (music), *geometria* (geometry), and *astrologia* (astronomy). This fourfold division of knowledge became known in the Middle Ages as the *quadrivium*, to which was added the *trivium* of logic, grammar, and rhetoric. These seven liberal arts came to be looked upon as the necessary course of study for an educated person.

Pythagoras divided those who attended his lectures into two groups: the Probationers (or listeners) and the Pythagoreans. After three years in the first class, a listener could be initiated into the second class, to whom were confided the main discoveries of the school. The Pythagoreans were a closely knit brotherhood, holding all worldly goods in common and bound by an oath not to reveal the founder's secrets. Legend has it that a talkative Pythagorean was drowned in a shipwreck as the gods' punishment for publicly boasting that he had added the dodecahedron to the number of regular solids enumerated by Pythagoras. For a time, the autocratic Pythagoreans succeeded in dominating the local government in Croton, but a popular revolt in 501 B.C. led to the murder of many of its prominent members, and Pythagoras himself was killed shortly thereafter. Although the political influence of the Pythagoreans thus was destroyed, they continued to exist for at least two centuries more as a philosophical and mathematical society. To the end, they remained a secret order, publishing nothing and, with noble self-denial, ascribing all their discoveries to the Master.

The Pythagoreans believed that the key to an explanation of the universe lay in number and form, their general thesis being that "Everything is Number." (By number, they meant, of course, a positive integer.) For a rational understanding of nature, they considered it sufficient to analyze the properties of certain numbers. Pythagoras himself, we are told "seems to have attached supreme importance to the study of arithmetic, which he advanced and took out of the realm of commercial utility."

The Pythagorean doctrine is a curious mixture of cosmic philosophy and number mysticism, a sort of supernumerology that assigned to everything material or spiritual a definite integer. Among their writings, we find that 1 represented reason, for reason could produce only one consistent body of truth; 2 stood for man and 3 for woman; 4 was the Pythagorean symbol for justice, being the first number that is the product of equals; 5 was identified with marriage, because it is formed by the union of 2 and 3; and so forth. All the even numbers, after the first one, were capable of separation into other numbers; hence, they were prolific and were considered as feminine and earthy—and somewhat less highly regarded in general. Being a predominantly male society, the Pythagoreans classified the odd numbers, after the first two, as masculine and divine.

Although these speculations about numbers as models of "things" appear frivolous today, it must be borne in mind that the intellectuals of the classical Greek period were largely absorbed in philosophy and that these same men, because they had such intellectual interests, were the very ones who were engaged in laying the foundations for mathematics as a system of thought. To Pythagoras and his followers, mathematics was largely a means to an end, the end being philosophy. Only with the founding of the School of Alexandria do we enter a new phase in which the cultivation of mathematics was pursued for its own sake.

It was at Alexandria, not Athens, that a science of numbers divorced from mystic philosophy first began to develop. For nearly a thousand years, until its destruction by the Arabs in 641 A.D., Alexandria stood at the cultural and commercial center of the Hellenistic world. (After the fall of Alexandria, most of its scholars migrated to Constantinople. During the next 800 years, while formal learning in the West all but disappeared, this enclave at Constantinople preserved for us the mathematical works of the various Greek schools.) The so-called Alexandrian Museum, a forerunner of the modern university, brought together the leading poets and scholars of the day; adjacent to it there was established an enormous library, reputed to hold over 700,000 volumes—hand-copied—at its height. Of all the distinguished names connected with the museum, that of Euclid (fl. c.300 B.C.), founder of the School of Mathematics, is in a special class. Posterity has come to know him as the author of the *Elements*, the oldest Greek treatise on mathematics to reach us in its entirety. The *Elements* is a compilation of much of the mathematical knowledge available at that time, organized into 13 parts or Books, as they are called. The name of Euclid is so often associated with geometry that one tends to forget that three of the Books—VII, VIII, and IX—are devoted to number theory.

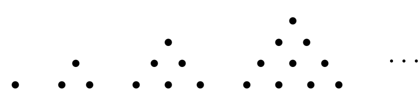
Euclid's *Elements* constitutes one of the great success stories of world literature. Scarcely any other book save the Bible has been more widely circulated or studied. Over a thousand editions of it have appeared since the first printed version in 1482, and before its printing, manuscript copies dominated much of the teaching of mathematics in Western Europe. Unfortunately, no copy of the work has been found that actually dates from Euclid's own time; the modern editions are descendants of a revision prepared by Theon of Alexandria, a commentator of the 4th century A.D.

PROBLEMS 2.1

1. Each of the numbers

$$1 = 1, 3 = 1 + 2, 6 = 1 + 2 + 3, 10 = 1 + 2 + 3 + 4, \dots$$

represents the number of dots that can be arranged evenly in an equilateral triangle:



This led the ancient Greeks to call a number *triangular* if it is the sum of consecutive integers, beginning with 1. Prove the following facts concerning triangular numbers:

(a) A number is triangular if and only if it is of the form $n(n+1)/2$ for some $n \geq 1$. (Pythagoras, circa 550 B.C.)

(b) The integer n is a triangular number if and only if $8n + 1$ is a perfect square. (Plutarch, circa 100 A.D.)

(c) The sum of any two consecutive triangular numbers is a perfect square. (Nicomachus, circa 100 A.D.)

(d) If n is a triangular number, then so are $9n + 1$, $25n + 3$, and $49n + 6$. (Euler, 1775)

2. If t_n denotes the nth triangular number, prove that in terms of the binomial coefficients,

$$t_n = \binom{n+1}{2} \qquad n \geq 1$$

3. Derive the following formula for the sum of triangular numbers, attributed to the Hindu mathematician Aryabhata (circa 500 A.D.):

$$t_1 + t_2 + t_3 + \cdots + t_n = \frac{n(n+1)(n+2)}{6} \qquad n \geq 1$$

[*Hint:* Group the terms on the left-hand side in pairs, noting the identity $t_{k-1} + t_k = k^2$.]

4. Prove that the square of any odd multiple of 3 is the difference of two triangular numbers; specifically, that

$$9(2n+1)^2 = t_{9n+4} - t_{3n+1}$$

5. In the sequence of triangular numbers, find the following:
(a) Two triangular numbers whose sum and difference are also triangular numbers.
(b) Three successive triangular numbers whose product is a perfect square.
(c) Three successive triangular numbers whose sum is a perfect square.

6. (a) If the triangular number t_n is a perfect square, prove that $t_{4n(n+1)}$ is also a square.
(b) Use part (a) to find three examples of squares that are also triangular numbers.

7. Show that the difference between the squares of two consecutive triangular numbers is always a cube.

8. Prove that the sum of the reciprocals of the first n triangular numbers is less than 2; that is,

$$\frac{1}{1} + \frac{1}{3} + \frac{1}{6} + \frac{1}{10} + \cdots + \frac{1}{t_n} < 2$$

[*Hint:* Observe that $\frac{2}{n(n+1)} = 2(\frac{1}{n} - \frac{1}{n+1})$.]

9. (a) Establish the identity $t_x = t_y + t_z$, where

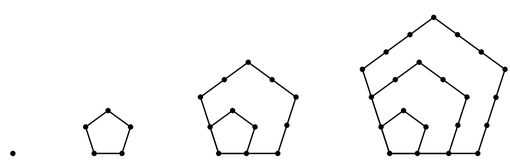
$$x = \frac{n(n+3)}{2} + 1 \qquad y = n+1 \qquad z = \frac{n(n+3)}{2}$$

and $n \geq 1$, thereby proving that there are infinitely many triangular numbers that are the sum of two other such numbers.
(b) Find three examples of triangular numbers that are sums of two other triangular numbers.

10. Each of the numbers

$$1, 5 = 1 + 4, 12 = 1 + 4 + 7, 22 = 1 + 4 + 7 + 10, \ldots$$

represents the number of dots that can be arranged evenly in a pentagon:



The ancient Greeks called these *pentagonal* numbers. If p_n denotes the nth pentagonal number, where $p_1 = 1$ and $p_n = p_{n-1} + (3n-2)$ for $n \geq 2$, prove that

$$p_n = \frac{n(3n-1)}{2}, \qquad n \geq 1$$

11. For $n \geq 2$, verify the following relations between the pentagonal, square, and triangular numbers:
(a) $p_n = t_{n-1} + n^2$
(b) $p_n = 3t_{n-1} + n = 2t_{n-1} + t_n$

2.2 THE DIVISION ALGORITHM

We have been exposed to relationships between integers for several pages and, as yet, not a single divisibility property has been derived. It is time to remedy this situation. One theorem, the Division Algorithm, acts as the foundation stone upon which our whole development rests. The result is familiar to most of us; roughly, it asserts that an integer a can be "divided" by a positive integer b in such a way that the remainder is smaller than is b. The exact statement of this fact is Theorem 2.1.

Theorem 2.1 Division Algorithm. Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

$$a = qb + r \qquad 0 \le r < b$$

The integers q and r are called, respectively, the *quotient* and *remainder* in the division of a by b.

Proof. We begin by proving that the set

$$S = \{a - xb \mid x \text{ an integer; } a - xb \ge 0\}$$

is nonempty. To do this, it suffices to exhibit a value of x making $a - xb$ nonnegative. Because the integer $b \ge 1$, we have $|a|b \ge |a|$, and so

$$a - (-|a|)b = a + |a|b \ge a + |a| \ge 0$$

For the choice $x = -|a|$, then, $a - xb$ lies in S. This paves the way for an application of the Well-Ordering Principle (Chapter 1), from which we infer that the set S contains a smallest integer; call it r. By the definition of S, there exists an integer q satisfying

$$r = a - qb \qquad 0 \le r$$

We argue that $r < b$. If this were not the case, then $r \ge b$ and

$$a - (q + 1)b = (a - qb) - b = r - b \ge 0$$

The implication is that the integer $a - (q + 1)b$ has the proper form to belong to the set S. But $a - (q + 1)b = r - b < r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r < b$.

Next we turn to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form, say,

$$a = qb + r = q'b + r'$$

where $0 \le r < b$, $0 \le r' < b$. Then $r' - r = b(q - q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$|r' - r| = b\,|q - q'|$$

Upon adding the two inequalities $-b < -r \le 0$ and $0 \le r' < b$, we obtain $-b < r' - r < b$ or, in equivalent terms, $|r' - r| < b$. Thus, $b\,|q - q'| < b$, which yields

$$0 \le |q - q'| < 1$$

Because $|q - q'|$ is a nonnegative integer, the only possibility is that $|q - q'| = 0$, whence $q = q'$; this, in turn, gives $r = r'$, ending the proof.

A more general version of the Division Algorithm is obtained on replacing the restriction that b must be positive by the simple requirement that $b \neq 0$.

Corollary. If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that

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

Proof. It is enough to consider the case in which b is negative. Then $|\, b\,| > 0$, and Theorem 2.1 produces unique integers q' and r for which

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

Noting that $|\, b\,| = -b$, we may take $q = -q'$ to arrive at $a = qb + r$, with $0 \leq r < |\, b\,|$.

To illustrate the Division Algorithm when $b < 0$, let us take $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59, we obtain the expressions

$$\begin{aligned} 1 &= 0(-7) + 1 \\ -2 &= 1(-7) + 5 \\ 61 &= (-8)(-7) + 5 \\ -59 &= 9(-7) + 4 \end{aligned}$$

We wish to focus our attention on the applications of the Division Algorithm, and not so much on the algorithm itself. As a first illustration, note that with $b = 2$ the possible remainders are $r = 0$ and $r = 1$. When $r = 0$, the integer a has the form $a = 2q$ and is called *even*; when $r = 1$, the integer a has the form $a = 2q + 1$ and is called *odd*. Now a^2 is either of the form $(2q)^2 = 4k$ or $(2q + 1)^2 = 4(q^2 + q) + 1 = 4k + 1$. The point to be made is that the square of an integer leaves the remainder 0 or 1 upon division by 4.

We also can show the following: the square of any odd integer is of the form $8k + 1$. For, by the Division Algorithm, any integer is representable as one of the four forms: $4q$, $4q + 1$, $4q + 2$, $4q + 3$. In this classification, only those integers of the forms $4q + 1$ and $4q + 3$ are odd. When the latter are squared, we find that

$$(4q + 1)^2 = 8(2q^2 + q) + 1 = 8k + 1$$

and similarly

$$(4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8k + 1$$

As examples, the square of the odd integer 7 is $7^2 = 49 = 8 \cdot 6 + 1$, and the square of 13 is $13^2 = 169 = 8 \cdot 21 + 1$.

As these remarks indicate, the advantage of the Division Algorithm is that it allows us to prove assertions about all the integers by considering only a finite number of cases. Let us illustrate this with one final example.

Example 2.1. We propose to show that the expression $a(a^2 + 2)/3$ is an integer for all $a \geq 1$. According to the Division Algorithm, every a is of the form $3q$, $3q + 1$, or

$3q + 2$. Assume the first of these cases. Then

$$\frac{a(a^2+2)}{3} = q(9q^2+2)$$

which clearly is an integer. Similarly, if $a = 3q + 1$, then

$$\frac{(3q+1)((3q+1)^2+2)}{3} = (3q+1)(3q^2+2q+1)$$

and $a(a^2 + 2)/3$ is an integer in this instance also. Finally, for $a = 3q + 2$, we obtain

$$\frac{(3q+2)((3q+2)^2+2)}{3} = (3q+2)(3q^2+4q+2)$$

an integer once more. Consequently, our result is established in all cases.

PROBLEMS 2.2

1. Prove that if a and b are integers, with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \le r < 3b$.
2. Show that any integer of the form $6k + 5$ is also of the form $3j + 2$, but not conversely.
3. Use the Division Algorithm to establish the following:
(a) The square of any integer is either of the form $3k$ or $3k + 1$.
(b) The cube of any integer has one of the forms: $9k$, $9k + 1$, or $9k + 8$.
(c) The fourth power of any integer is either of the form $5k$ or $5k + 1$.
4. Prove that $3a^2 - 1$ is never a perfect square.
[*Hint:* Problem 3(a).]
5. For $n \ge 1$, prove that $n(n + 1)(2n + 1)/6$ is an integer.
[*Hint:* By the Division Algorithm, n has one of the forms $6k, 6k + 1, \dots, 6k + 5$; establish the result in each of these six cases.]
6. Show that the cube of any integer is of the form $7k$ or $7k \pm 1$.
7. Obtain the following version of the Division Algorithm: For integers a and b, with $b \ne 0$, there exist unique integers q and r that satisfy $a = qb + r$, where $-\frac{1}{2}|b| < r \le \frac{1}{2}|b|$.
[*Hint:* First write $a = q'b + r'$, where $0 \le r' < |b|$. When $0 \le r' \le \frac{1}{2}|b|$, let $r = r'$ and $q = q'$; when $\frac{1}{2}|b| < r' < |b|$, let $r = r' - |b|$ and $q = q' + 1$ if $b > 0$ or $q = q' - 1$ if $b < 0$.]
8. Prove that no integer in the following sequence is a perfect square:

$$11, 111, 1111, 11111, \dots$$

[*Hint:* A typical term $111\cdots111$ can be written as

$$111\cdots111 = 111\cdots108 + 3 = 4k + 3.]$$

9. Verify that if an integer is simultaneously a square and a cube (as is the case with $64 = 8^2 = 4^3$), then it must be either of the form $7k$ or $7k + 1$.
10. For $n \ge 1$, establish that the integer $n(7n^2 + 5)$ is of the form $6k$.
11. If n is an odd integer, show that $n^4 + 4n^2 + 11$ is of the form $16k$.

2.3 THE GREATEST COMMON DIVISOR

Of special significance is the case in which the remainder in the Division Algorithm turns out to be zero. Let us look into this situation now.

Definition 2.1. An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Thus, for example, -12 is divisible by 4, because $-12 = 4(-3)$. However, 10 is not divisible by 3; for there is no integer c that makes the statement $10 = 3c$ true.

There is other language for expressing the divisibility relation $a \mid b$. We could say that a is a *divisor* of b, that a is a *factor* of b, or that b is a *multiple* of a. Notice that in Definition 2.1 there is a restriction on the divisor a: whenever the notation $a \mid b$ is employed, it is understood that a is different from zero.

If a is a divisor of b, then b is also divisible by $-a$ (indeed, $b = ac$ implies that $b = (-a)(-c)$), so that the divisors of an integer always occur in pairs. To find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers. For this reason, we shall usually limit ourselves to a consideration of positive divisors.

It will be helpful to list some immediate consequences of Definition 2.1. (The reader is again reminded that, although not stated, divisors are assumed to be nonzero.)

Theorem 2.2. For integers a, b, c, the following hold:

(a) $a \mid 0$, $1 \mid a$, $a \mid a$.
(b) $a \mid 1$ if and only if $a = \pm 1$.
(c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
(d) If $a \mid b$ and $b \mid c$, then $a \mid c$.
(e) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.
(f) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.
(g) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.

Proof. We shall prove assertions (f) and (g), leaving the other parts as an exercise. If $a \mid b$, then there exists an integer c such that $b = ac$; also, $b \neq 0$ implies that $c \neq 0$. Upon taking absolute values, we get $|b| = |ac| = |a||c|$. Because $c \neq 0$, it follows that $|c| \geq 1$, whence $|b| = |a||c| \geq |a|$.

As regards (g), the relations $a \mid b$ and $a \mid c$ ensure that $b = ar$ and $c = as$ for suitable integers r and s. But then whatever the choice of x and y,

$$bx + cy = arx + asy = a(rx + sy)$$

Because $rx + sy$ is an integer, this says that $a \mid (bx + cy)$, as desired.

It is worth pointing out that property (g) of Theorem 2.2 extends by induction to sums of more than two terms. That is, if $a \mid b_k$ for $k = 1, 2, \ldots, n$, then

$$a \mid (b_1x_1 + b_2x_2 + \cdots + b_nx_n)$$

for all integers $x_1, x_2, \ldots, x_n$. The few details needed for the proof are so straightforward that we omit them.

If a and b are arbitrary integers, then an integer d is said to be a *common divisor* of a and b if both $d \mid a$ and $d \mid b$. Because 1 is a divisor of every integer, 1 is a common divisor of a and b; hence, their set of positive common divisors is nonempty. Now every integer divides zero, so that if $a = b = 0$, then every integer serves as a common divisor of a and b. In this instance, the set of positive common divisors of a and b is infinite. However, when at least one of a or b is different from zero, there are only a finite number of positive common divisors. Among these, there is a largest one, called the greatest common divisor of a and b. We frame this as Definition 2.2.

Definition 2.2. Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following:

(a) $d \mid a$ and $d \mid b$.
(b) If $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 2.2. The positive divisors of -12 are 1, 2, 3, 4, 6, 12, whereas those of 30 are 1, 2, 3, 5, 6, 10, 15, 30; hence, the positive common divisors of -12 and 30 are 1, 2, 3, 6. Because 6 is the largest of these integers, it follows that $\gcd(-12, 30) = 6$. In the same way, we can show that

$$\gcd(-5, 5) = 5 \qquad \gcd(8, 17) = 1 \qquad \gcd(-8, -36) = 4$$

The next theorem indicates that $\gcd(a, b)$ can be represented as a linear combination of a and b. (By a *linear combination* of a and b, we mean an expression of the form $ax + by$, where x and y are integers.) This is illustrated by, say,

$$\gcd(-12, 30) = 6 = (-12)2 + 30 \cdot 1$$

or

$$\gcd(-8, -36) = 4 = (-8)4 + (-36)(-1)$$

Now for the theorem.

Theorem 2.3. Given integers a and b, not both of which are zero, there exist integers x and y such that

$$\gcd(a, b) = ax + by$$

Proof. Consider the set S of all positive linear combinations of a and b:

$$S = \{au + bv \mid au + bv > 0; u, v \text{ integers}\}$$

Notice first that S is not empty. For example, if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ lies in S, where we choose $u = 1$ or $u = -1$ according as a is positive or negative. By virtue of the Well-Ordering Principle, S must contain a smallest element d. Thus, from the very definition of S, there exist integers x and y for which $d = ax + by$. We claim that $d = \gcd(a, b)$.

Taking stock of the Division Algorithm, we can obtain integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form

$$\begin{aligned} r = a - qd &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

If r were positive, then this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S (recall that $r < d$). Therefore, $r = 0$, and so $a = qd$, or equivalently $d \mid a$. By similar reasoning, $d \mid b$, the effect of which is to make d a common divisor of a and b.

Now if c is an arbitrary positive common divisor of the integers a and b, then part (g) of Theorem 2.2 allows us to conclude that $c \mid (ax + by)$; that is, $c \mid d$. By part (f) of the same theorem, $c = |c| \leq |d| = d$, so that d is greater than every positive common divisor of a and b. Piecing the bits of information together, we see that $d = \gcd(a, b)$.

It should be noted that the foregoing argument is merely an "existence" proof and does not provide a practical method for finding the values of x and y. This will come later.

A perusal of the proof of Theorem 2.3 reveals that the greatest common divisor of a and b may be described as the smallest positive integer of the form $ax + by$. Consider the case in which $a = 6$ and $b = 15$. Here, the set S becomes

$$\begin{aligned} S &= \{6(-2) + 15 \cdot 1, 6(-1) + 15 \cdot 1, 6 \cdot 1 + 15 \cdot 0, \ldots\} \\ &= \{3, 9, 6, \ldots\} \end{aligned}$$

We observe that 3 is the smallest integer in S, whence $3 = \gcd(6, 15)$.

The nature of the members of S appearing in this illustration suggests another result, which we give in the next corollary.

Corollary. If a and b are given integers, not both zero, then the set

$$T = \{ax + by \mid x, y \text{ are integers}\}$$

is precisely the set of all multiples of $d = \gcd(a, b)$.

Proof. Because $d \mid a$ and $d \mid b$, we know that $d \mid (ax + by)$ for all integers x, y. Thus, every member of T is a multiple of d. Conversely, d may be written as $d = ax_0 + by_0$ for suitable integers x_0 and y_0, so that any multiple nd of d is of the form

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0)$$

Hence, nd is a linear combination of a and b, and, by definition, lies in T.

It may happen that 1 and -1 are the only common divisors of a given pair of integers a and b, whence $\gcd(a, b) = 1$. For example:

$$\gcd(2, 5) = \gcd(-9, 16) = \gcd(-27, -35) = 1$$

This situation occurs often enough to prompt a definition.

Definition 2.3. Two integers a and b, not both of which are zero, are said to be *relatively prime* whenever $\gcd(a, b) = 1$.

The following theorem characterizes relatively prime integers in terms of linear combinations.

Theorem 2.4. Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Proof. If a and b are relatively prime so that $\gcd(a, b) = 1$, then Theorem 2.3 guarantees the existence of integers x and y satisfying $1 = ax + by$. As for the converse, suppose that $1 = ax + by$ for some choice of x and y, and that $d = \gcd(a, b)$. Because $d \mid a$ and $d \mid b$, Theorem 2.2 yields $d \mid (ax + by)$, or $d \mid 1$. Inasmuch as d is a positive integer, this last divisibility condition forces d to equal 1 (part (b) of Theorem 2.2 plays a role here), and the desired conclusion follows.

This result leads to an observation that is useful in certain situations; namely,

Corollary 1. If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.

Proof. Before starting with the proof proper, we should observe that although a/d and b/d have the appearance of fractions, in fact, they are integers because d is a divisor both of a and of b. Now, knowing that $\gcd(a, b) = d$, it is possible to find integers x and y such that $d = ax + by$. Upon dividing each side of this equation by d, we obtain the expression

$$1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y$$

Because a/d and b/d are integers, an appeal to the theorem is legitimate. The conclusion is that a/d and b/d are relatively prime.

For an illustration of the last corollary, let us observe that $\gcd(-12, 30) = 6$ and

$$\gcd(-12/6, 30/6) = \gcd(-2, 5) = 1$$

as it should be.

It is not true, without adding an extra condition, that $a \mid c$ and $b \mid c$ together give $ab \mid c$. For instance, $6 \mid 24$ and $8 \mid 24$, but $6 \cdot 8 \nmid 24$. If 6 and 8 were relatively prime, of course, this situation would not arise. This brings us to Corollary 2.

Corollary 2. If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.

Proof. Inasmuch as $a \mid c$ and $b \mid c$, integers r and s can be found such that $c = ar = bs$. Now the relation $\gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y. Multiplying the last equation by c, it appears that

$$c = c \cdot 1 = c(ax + by) = acx + bcy$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

or, as a divisibility statement, $ab \mid c$.

Our next result seems mild enough, but is of fundamental importance.

Theorem 2.5 Euclid's lemma. If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.

Proof. We start again from Theorem 2.3, writing $1 = ax + by$, where x and y are integers. Multiplication of this equation by c produces

$$c = 1 \cdot c = (ax + by)c = acx + bcy$$

Because $a \mid ac$ and $a \mid bc$, it follows that $a \mid (acx + bcy)$, which can be recast as $a \mid c$.

If a and b are not relatively prime, then the conclusion of Euclid's lemma may fail to hold. Here is a specific example: $12 \mid 9 \cdot 8$, but $12 \nmid 9$ and $12 \nmid 8$.

The subsequent theorem often serves as a definition of $\gcd(a, b)$. The advantage of using it as a definition is that order relationship is not involved. Thus, it may be used in algebraic systems having no order relation.

Theorem 2.6. Let a, b be integers, not both zero. For a positive integer d, $d = \gcd(a, b)$ if and only if

(a) $d \mid a$ and $d \mid b$.
(b) Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. To begin, suppose that $d = \gcd(a, b)$. Certainly, $d \mid a$ and $d \mid b$, so that (a) holds. In light of Theorem 2.3, d is expressible as $d = ax + by$ for some integers x, y. Thus, if $c \mid a$ and $c \mid b$, then $c \mid (ax + by)$, or rather $c \mid d$. In short, condition (b) holds. Conversely, let d be any positive integer satisfying the stated conditions. Given any common divisor c of a and b, we have $c \mid d$ from hypothesis (b). The implication is that $d \geq c$, and consequently d is the greatest common divisor of a and b.

PROBLEMS 2.3

1. If $a \mid b$, show that $(-a) \mid b$, $a \mid (-b)$, and $(-a) \mid (-b)$.
2. Given integers a, b, c, d, verify the following:
   (a) If $a \mid b$, then $a \mid bc$.
   (b) If $a \mid b$ and $a \mid c$, then $a^2 \mid bc$.
   (c) $a \mid b$ if and only if $ac \mid bc$, where $c \neq 0$.
   (d) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
3. Prove or disprove: If $a \mid (b + c)$, then either $a \mid b$ or $a \mid c$.
4. For $n \geq 1$, use mathematical induction to establish each of the following divisibility statements:
   (a) $8 \mid 5^{2n} + 7$.
   [*Hint:* $5^{2(k+1)} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 \cdot 7)$.]
   (b) $15 \mid 2^{4n} - 1$.
   (c) $5 \mid 3^{3n+1} + 2^{n+1}$.
   (d) $21 \mid 4^{n+1} + 5^{2n-1}$.
   (e) $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$.
5. Prove that for any integer a, one of the integers a, $a + 2$, $a + 4$ is divisible by 3.

6. For an arbitrary integer a, verify the following:
(a) $2 \mid a(a+1)$, and $3 \mid a(a+1)(a+2)$.
(b) $3 \mid a(2a^2+7)$.
(c) If a is odd, then $32 \mid (a^2+3)(a^2+7)$.
7. Prove that if a and b are both odd integers, then $16 \mid a^4 + b^4 - 2$.
8. Prove the following:
(a) The sum of the squares of two odd integers cannot be a perfect square.
(b) The product of four consecutive integers is 1 less than a perfect square.
9. Establish that the difference of two consecutive cubes is never divisible by 2.
10. For a nonzero integer a, show that $\gcd(a, 0) = |a|$, $\gcd(a, a) = |a|$, and $\gcd(a, 1) = 1$.
11. If a and b are integers, not both of which are zero, verify that

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$$

12. Prove that, for a positive integer n and any integer a, $\gcd(a, a+n)$ divides n; hence, $\gcd(a, a+1) = 1$.
13. Given integers a and b, prove the following:
(a) There exist integers x and y for which $c = ax + by$ if and only if $\gcd(a, b) \mid c$.
(b) If there exist integers x and y for which $ax + by = \gcd(a, b)$, then $\gcd(x, y) = 1$.
14. For any integer a, show the following:
(a) $\gcd(2a+1, 9a+4) = 1$.
(b) $\gcd(5a+2, 7a+3) = 1$.
(c) If a is odd, then $\gcd(3a, 3a+2) = 1$.
15. If a and b are integers, not both of which are zero, prove that $\gcd(2a-3b, 4a-5b)$ divides b; hence, $\gcd(2a+3, 4a+5) = 1$.
16. Given an odd integer a, establish that

$$a^2 + (a+2)^2 + (a+4)^2 + 1$$

is divisible by 12.
17. Prove that the expression $(3n)!/(3!)^n$ is an integer for all $n \geq 0$.
18. Prove: The product of any three consecutive integers is divisible by 6; the product of any four consecutive integers is divisible by 24; the product of any five consecutive integers is divisible by 120.
[*Hint:* See Corollary 2 to Theorem 2.4.]
19. Establish each of the assertions below:
(a) If a is an arbitrary integer, then $6 \mid a(a^2+11)$.
(b) If a is an odd integer, then $24 \mid a(a^2-1)$.
[*Hint:* The square of an odd integer is of the form $8k+1$.]
(c) If a and b are odd integers, then $8 \mid (a^2 - b^2)$.
(d) If a is an integer not divisible by 2 or 3, then $24 \mid (a^2 + 23)$.
(e) If a is an arbitrary integer, then $360 \mid a^2(a^2-1)(a^2-4)$.
20. Confirm the following properties of the greatest common divisor:
(a) If $\gcd(a, b) = 1$, and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
[*Hint:* Because $1 = ax + by = au + cv$ for some x, y, u, v,
$1 = (ax+by)(au+cv) = a(aux + cvx + byu) + bc(yv)$.]
(b) If $\gcd(a, b) = 1$, and $c \mid a$, then $\gcd(b, c) = 1$.
(c) If $\gcd(a, b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$.
(d) If $\gcd(a, b) = 1$, and $c \mid a + b$, then $\gcd(a, c) = \gcd(b, c) = 1$.
[*Hint:* Let $d = \gcd(a, c)$. Then $d \mid a$, $d \mid c$ implies that $d \mid (a+b) - a$, or $d \mid b$.]
(e) If $\gcd(a, b) = 1$, $d \mid ac$, and $d \mid bc$, then $d \mid c$.
(f) If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.
[*Hint:* First show that $\gcd(a, b^2) = \gcd(a^2, b) = 1$.]

21. (a) Prove that if $d \mid n$, then $2^d - 1 \mid 2^n - 1$.
[*Hint:* Use the identity
$$x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1).]$$
(b) Verify that $2^{35} - 1$ is divisible by 31 and 127.

22. Let t_n denote the nth triangular number. For what values of n does t_n divide the sum $t_1 + t_2 + \cdots + t_n$?
[*Hint:* See Problem 1(c), Section 1.1.]

23. If $a \mid bc$, show that $a \mid \gcd(a, b)\gcd(a, c)$.

2.4 THE EUCLIDEAN ALGORITHM

The greatest common divisor of two integers can be found by listing all their positive divisors and choosing the largest one common to each; but this is cumbersome for large numbers. A more efficient process, involving repeated application of the Division Algorithm, is given in the seventh book of the *Elements*. Although there is historical evidence that this method predates Euclid, today it is referred to as the *Euclidean Algorithm*.

The Euclidean Algorithm may be described as follows: Let a and b be two integers whose greatest common divisor is desired. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming that $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to get
$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$
If it happens that $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying
$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$
If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain
$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$
This division process continues until some zero remainder appears, say, at the $(n+1)$th stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers).

The result is the following system of equations:
$$\begin{aligned}
a &= q_1 b + r_1 & 0 &< r_1 < b \\
b &= q_2 r_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &< r_3 < r_2 \\
&\ \vdots \\
r_{n-2} &= q_n r_{n-1} + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$
We argue that r_n, the last nonzero remainder that appears in this manner, is equal to $\gcd(a, b)$. Our proof is based on the lemma below.

Lemma. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. If $d = \gcd(a, b)$, then the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - qb)$, or $d \mid r$. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c \mid (qb + r)$, whence $c \mid a$. This makes c a common divisor of a and b, so that $c \leq d$. It now follows from the definition of $\gcd(b, r)$ that $d = \gcd(b, r)$.

Using the result of this lemma, we simply work down the displayed system of equations, obtaining

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

as claimed.

Theorem 2.3 asserts that $\gcd(a, b)$ can be expressed in the form $ax + by$, but the proof of the theorem gives no hint as to how to determine the integers x and y. For this, we fall back on the Euclidean Algorithm. Starting with the next-to-last equation arising from the algorithm, we write

$$r_n = r_{n-2} - q_n r_{n-1}$$

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain

$$\begin{aligned} r_n &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= (1 + q_n q_{n-1})r_{n-2} + (-q_n)r_{n-3} \end{aligned}$$

This represents r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing backward through the system of equations, we successively eliminate the remainders r_{n-1}, $r_{n-2}, \ldots, r_2, r_1$ until a stage is reached where $r_n = \gcd(a, b)$ is expressed as a linear combination of a and b.

Example 2.3. Let us see how the Euclidean Algorithm works in a concrete case by calculating, say, gcd(12378, 3054). The appropriate applications of the Division Algorithm produce the equations

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

Our previous discussion tells us that the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

$$6 = \gcd(12378, 3054)$$

To represent 6 as a linear combination of the integers 12378 and 3054, we start with the next-to-last of the displayed equations and successively eliminate the remainders

18, 24, 138, and 162:

$$\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (138 - 5 \cdot 24) \\
&= 6 \cdot 24 - 138 \\
&= 6(162 - 138) - 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\
&= 132 \cdot 162 - 7 \cdot 3054 \\
&= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\
&= 132 \cdot 12378 + (-535)3054
\end{aligned}$$

Thus, we have

$$6 = \gcd(12378, 3054) = 12378x + 3054y$$

where $x = 132$ and $y = -535$. Note that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054; among other possibilities, we could add and subtract $3054 \cdot 12378$ to get

$$\begin{aligned}
6 &= (132 + 3054)12378 + (-535 - 12378)3054 \\
&= 3186 \cdot 12378 + (-12913)3054
\end{aligned}$$

The French mathematician Gabriel Lamé (1795–1870) proved that the number of steps required in the Euclidean Algorithm is at most five times the number of digits in the smaller integer. In Example 2.3, the smaller integer (namely, 3054) has four digits, so that the total number of divisions cannot be greater than 20; in actuality only six divisions were needed. Another observation of interest is that for each $n > 0$, it is possible to find integers a_n and b_n such that exactly n divisions are required to compute $\gcd(a_n, b_n)$ by the Euclidean Algorithm. We shall prove this fact in Chapter 14.

One more remark is necessary. The number of steps in the Euclidean Algorithm usually can be reduced by selecting remainders r_{k+1} such that $|r_{k+1}| < r_k/2$, that is, by working with least absolute remainders in the divisions. Thus, repeating Example 2.3, it is more efficient to write

$$\begin{aligned}
12378 &= 4 \cdot 3054 + 162 \\
3054 &= 19 \cdot 162 - 24 \\
162 &= 7 \cdot 24 - 6 \\
24 &= (-4)(-6) + 0
\end{aligned}$$

As evidenced by this set of equations, this scheme is apt to produce the negative of the value of the greatest common divisor of two integers (the last nonzero remainder being -6), rather than the greatest common divisor itself.

An important consequence of the Euclidean Algorithm is the following theorem.

Theorem 2.7. If $k > 0$, then $\gcd(ka, kb) = k \gcd(a, b)$.

Proof. If each of the equations appearing in the Euclidean Algorithm for a and b (see page 28) is multiplied by k, we obtain

$$\begin{aligned}
ak &= q_1(bk) + r_1k & 0 &< r_1k < bk \\
bk &= q_2(r_1k) + r_2k & 0 &< r_2k < r_1k \\
&\vdots \\
r_{n-2}k &= q_n(r_{n-1}k) + r_nk & 0 &< r_nk < r_{n-1}k \\
r_{n-1}k &= q_{n+1}(r_nk) + 0
\end{aligned}$$

But this is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder r_nk; that is,

$$\gcd(ka, kb) = r_nk = k \gcd(a, b)$$

as stated in the theorem.

Corollary. For any integer $k \neq 0$, $\gcd(ka, kb) = |\,k\,| \gcd(a, b)$.

Proof. It suffices to consider the case in which $k < 0$. Then $-k = |\,k\,| > 0$ and, by Theorem 2.7,

$$\begin{aligned}
\gcd(ak, bk) &= \gcd(-ak, -bk) \\
&= \gcd(a\,|\,k\,|, b\,|\,k\,|) \\
&= |\,k\,| \gcd(a, b)
\end{aligned}$$

An alternate proof of Theorem 2.7 runs very quickly as follows: $\gcd(ak, bk)$ is the smallest positive integer of the form $(ak)x + (bk)y$, which, in turn, is equal to k times the smallest positive integer of the form $ax + by$; the latter value is equal to $k \gcd(a, b)$.

By way of illustrating Theorem 2.7, we see that

$$\gcd(12, 30) = 3 \gcd(4, 10) = 3 \cdot 2 \gcd(2, 5) = 6 \cdot 1 = 6$$

There is a concept parallel to that of the greatest common divisor of two integers, known as their least common multiple; but we shall not have much occasion to make use of it. An integer c is said to be a *common multiple* of two nonzero integers a and b whenever $a \mid c$ and $b \mid c$. Evidently, zero is a common multiple of a and b. To see there exist common multiples that are not trivial, just note that the products ab and $-(ab)$ are both common multiples of a and b, and one of these is positive. By the Well-Ordering Principle, the set of positive common multiples of a and b must contain a smallest integer; we call it the least common multiple of a and b.

For the record, here is the official definition.

Definition 2.4. The *least common multiple* of two nonzero integers a and b, denoted by $\operatorname{lcm}(a, b)$, is the positive integer m satisfying the following:

(a) $a \mid m$ and $b \mid m$.
(b) If $a \mid c$ and $b \mid c$, with $c > 0$, then $m \leq c$.

As an example, the positive common multiples of the integers -12 and 30 are 60, 120, 180, ...; hence, $\text{lcm}(-12, 30) = 60$.

The following remark is clear from our discussion: given nonzero integers a and b, $\text{lcm}(a, b)$ always exists and $\text{lcm}(a, b) \le |\,ab\,|$.

We lack a relationship between the ideas of greatest common divisor and least common multiple. This gap is filled by Theorem 2.8.

Theorem 2.8. For positive integers a and b

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

Proof. To begin, put $d = \gcd(a, b)$ and write $a = dr$, $b = ds$ for integers r and s. If $m = ab/d$, then $m = as = rb$, the effect of which is to make m a (positive) common multiple of a and b.

Now let c be any positive integer that is a common multiple of a and b; say, for definiteness, $c = au = bv$. As we know, there exist integers x and y satisfying $d = ax + by$. In consequence,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

This equation states that $m \mid c$, allowing us to conclude that $m \le c$. Thus, in accordance with Definition 2.4, $m = \text{lcm}(a, b)$; that is,

$$\text{lcm}(a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)}$$

which is what we started out to prove.

Theorem 2.8 has a corollary that is worth a separate statement.

Corollary. For any choice of positive integers a and b, $\text{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

Perhaps the chief virtue of Theorem 2.8 is that it makes the calculation of the least common multiple of two integers dependent on the value of their greatest common divisor—which, in turn, can be calculated from the Euclidean Algorithm. When considering the positive integers 3054 and 12378, for instance, we found that $\gcd(3054, 12378) = 6$; whence,

$$\text{lcm}(3054, 12378) = \frac{3054 \cdot 12378}{6} = 6300402$$

Before moving on to other matters, let us observe that the notion of greatest common divisor can be extended to more than two integers in an obvious way. In the case of three integers, a, b, c, not all zero, $\gcd(a, b, c)$ is defined to be the positive integer d having the following properties:

(a) d is a divisor of each of a, b, c.

(b) If e divides the integers a, b, c, then $e \le d$.

We cite two examples:

$$\gcd(39, 42, 54) = 3 \qquad \text{and} \qquad \gcd(49, 210, 350) = 7$$

The reader is cautioned that it is possible for three integers to be relatively prime as a triple (in other words, $\gcd(a, b, c) = 1$), yet not relatively prime in pairs; this is brought out by the integers 6, 10, and 15.

PROBLEMS 2.4

1. Find $\gcd(143, 227)$, $\gcd(306, 657)$, and $\gcd(272, 1479)$.
2. Use the Euclidean Algorithm to obtain integers x and y satisfying the following:
   (a) $\gcd(56, 72) = 56x + 72y$.
   (b) $\gcd(24, 138) = 24x + 138y$.
   (c) $\gcd(119, 272) = 119x + 272y$.
   (d) $\gcd(1769, 2378) = 1769x + 2378y$.
3. Prove that if d is a common divisor of a and b, then $d = \gcd(a, b)$ if and only if $\gcd(a/d, b/d) = 1$.
   [*Hint:* Use Theorem 2.7.]
4. Assuming that $\gcd(a, b) = 1$, prove the following:
   (a) $\gcd(a + b, a - b) = 1$ or 2.
   [*Hint:* Let $d = \gcd(a + b, a - b)$ and show that $d \mid 2a$, $d \mid 2b$, and thus that $d \leq \gcd(2a, 2b) = 2\gcd(a, b)$.]
   (b) $\gcd(2a + b, a + 2b) = 1$ or 3.
   (c) $\gcd(a + b, a^2 + b^2) = 1$ or 2.
   [*Hint:* $a^2 + b^2 = (a + b)(a - b) + 2b^2$.]
   (d) $\gcd(a + b, a^2 - ab + b^2) = 1$ or 3.
   [*Hint:* $a^2 - ab + b^2 = (a + b)^2 - 3ab$.]
5. For $n \geq 1$, and positive integers a, b, show the following:
   (a) If $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$.
   [*Hint:* See Problem 20(a), Section 2.2.]
   (b) The relation $a^n \mid b^n$ implies that $a \mid b$.
   [*Hint:* Put $d = \gcd(a, b)$ and write $a = rd$, $b = sd$, where $\gcd(r, s) = 1$. By part (a), $\gcd(r^n, s^n) = 1$. Show that $r = 1$, whence $a = d$.]
6. Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.
7. For nonzero integers a and b, verify that the following conditions are equivalent:
   (a) $a \mid b$.
   (b) $\gcd(a, b) = |a|$.
   (c) $\operatorname{lcm}(a, b) = |b|$.
8. Find $\operatorname{lcm}(143, 227)$, $\operatorname{lcm}(306, 657)$, and $\operatorname{lcm}(272, 1479)$.
9. Prove that the greatest common divisor of two positive integers divides their least common multiple.
10. Given nonzero integers a and b, establish the following facts concerning $\operatorname{lcm}(a, b)$:
    (a) $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = \pm b$.
    (b) If $k > 0$, then $\operatorname{lcm}(ka, kb) = k \operatorname{lcm}(a, b)$.
    (c) If m is any common multiple of a and b, then $\operatorname{lcm}(a, b) \mid m$.
    [*Hint:* Put $t = \operatorname{lcm}(a, b)$ and use the Division Algorithm to write $m = qt + r$, where $0 \leq r < t$. Show that r is a common multiple of a and b.]
11. Let a, b, c be integers, no two of which are zero, and $d = \gcd(a, b, c)$. Show that

$$d = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b)$$

12. Find integers x, y, z satisfying

$$\gcd(198, 288, 512) = 198x + 288y + 512z$$

[*Hint:* Put $d = \gcd(198, 288)$. Because $\gcd(198, 288, 512) = \gcd(d, 512)$, first find integers u and v for which $\gcd(d, 512) = du + 512v$.]

2.5 THE DIOPHANTINE EQUATION $ax + by = c$

We now change focus somewhat and take up the study of Diophantine equations. The name honors the mathematician Diophantus, who initiated the study of such equations. Practically nothing is known of Diophantus as an individual, save that he lived in Alexandria sometime around 250 A.D. The only positive evidence as to the date of his activity is that the Bishop of Laodicea, who began his episcopate in 270, dedicated a book on Egyptian computation to his friend Diophantus. Although Diophantus's works were written in Greek and he displayed the Greek genius for theoretical abstraction, he was most likely a Hellenized Babylonian. The only personal particulars we have of his career come from the wording of an epigram-problem (apparently dating from the 4th century): his boyhood lasted 1/6 of his life; his beard grew after 1/12 more; after 1/7 more he married, and his son was born 5 years later; the son lived to half his father's age and the father died 4 years after his son. If x was the age at which Diophantus died, these data lead to the equation

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x$$

with solution $x = 84$. Thus, he must have reached an age of 84, but in what year or even in what century is not certain.

The great work upon which the reputation of Diophantus rests is his *Arithmetica*, which may be described as the earliest treatise on algebra. Only six books of the original thirteen have been preserved. It is in the *Arithmetica* that we find the first systematic use of mathematical notation, although the signs employed are of the nature of abbreviations for words rather than algebraic symbols in the sense with which we use them today. Special symbols are introduced to represent frequently occurring concepts, such as the unknown quantity in an equation and the different powers of the unknown up to the sixth power; Diophantus also had a symbol to express subtraction, and another for equality.

The part of the *Arithmetica* that has come down to us consists of some 200 problems, which we could now express as equations, together with their worked-out solutions in specific numbers. Considerable attention was devoted to problems involving squares or cubes. Even for problems with infinitely many solutions, Diophantus was content with finding just one. Solutions were usually given in terms of positive rational numbers, sometimes admitting positive integers; there was no notion at that time of negative numbers as mathematical entities.

Although the *Arithmetica* does not fall into the realm of number theory, which involves properties of the integers, it nevertheless gave great impetus to subsequent European development of the subject. In the mid-17th century, the French mathematician Pierre de Fermat acquired a Latin translation of the rediscovered books of

Diophantus's treatise. Fermat embarked on a careful study of its solution techniques, looking for integral solutions to replace the rational ones of Diophantus and opening up new paths at which the *Arithmetica* only hinted. As an example, one problem asked the following: find four numbers such that the product of any two, increased by 1, is a square. Diophantus's methods had led him to the set $\frac{1}{16}, \frac{33}{16}, \frac{68}{16}, \frac{105}{16}$; but Fermat produced the four positive integers 1, 3, 8, 120. (Another set is 3, 8, 21, 2081.)

The *Arithmetica* became a treasure trove for later number theorists. Through the years, mathematicians have been intrigued by such problems, extending and generalizing them in one way and another. Consider, for instance, Diophantus's problem of finding three numbers such that the product of any two, increased by the sum of the same two, is a square. In the 18th century, Leonhard Euler treated the same problem with four numbers; and recently a set of five numbers with the indicated property has been found. To this day the *Arithmetica* remains a source of inspiration to number theorists.

It is customary to apply the term *Diophantine equation* to any equation in one or more unknowns that is to be solved in the integers. The simplest type of Diophantine equation that we shall consider is the linear Diophantine equation in two unknowns:

$$ax + by = c$$

where a, b, c are given integers and a, b are not both zero. A solution of this equation is a pair of integers x_0, y_0 that, when substituted into the equation, satisfy it; that is, we ask that $ax_0 + by_0 = c$. Curiously enough, the linear equation does not appear in the extant works of Diophantus (the theory required for its solution is to be found in Euclid's *Elements*), possibly because he viewed it as trivial; most of his problems deal with finding squares or cubes with certain properties.

A given linear Diophantine equation can have a number of solutions, as is the case with $3x + 6y = 18$, where

$$\begin{aligned} 3 \cdot 4 + 6 \cdot 1 &= 18 \\ 3(-6) + 6 \cdot 6 &= 18 \\ 3 \cdot 10 + 6(-2) &= 18 \end{aligned}$$

By contrast, there is no solution to the equation $2x + 10y = 17$. Indeed, the left-hand side is an even integer whatever the choice of x and y, whereas the right-hand side is not. Faced with this, it is reasonable to enquire about the circumstances under which a solution is possible and, when a solution does exist, whether we can determine all solutions explicitly.

The condition for solvability is easy to state: the linear Diophantine equation $ax + by = c$ admits a solution if and only if $d \mid c$, where $d = \gcd(a, b)$. We know that there are integers r and s for which $a = dr$ and $b = ds$. If a solution of $ax + by = c$ exists, so that $ax_0 + by_0 = c$ for suitable x_0 and y_0, then

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$$

which simply says that $d \mid c$. Conversely, assume that $d \mid c$, say $c = dt$. Using Theorem 2.3, integers x_0 and y_0 can be found satisfying $d = ax_0 + by_0$. When this relation is multiplied by t, we get

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$$

Hence, the Diophantine equation $ax + by = c$ has $x = tx_0$ and $y = ty_0$ as a particular solution. This proves part of our next theorem.

Theorem 2.9. The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

where t is an arbitrary integer.

Proof. To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

$$ax_0 + by_0 = c = ax' + by'$$

which is equivalent to

$$a(x' - x_0) = b(y_0 - y')$$

By the corollary to Theorem 2.4, there exist relatively prime integers r and s such that $a = dr$, $b = ds$. Substituting these values into the last-written equation and canceling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y')$$

The situation is now this: $r \mid s(y_0 - y')$, with $\gcd(r, s) = 1$. Using Euclid's lemma, it must be the case that $r \mid (y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some integer t. Substituting, we obtain

$$x' - x_0 = st$$

This leads us to the formulas

$$x' = x_0 + st = x_0 + \left(\frac{b}{d}\right)t$$

$$y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right)t$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for

$$\begin{aligned} ax' + by' &= a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{d}\right)t\right] \\ &= (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t \\ &= c + 0 \cdot t \\ &= c \end{aligned}$$

Thus, there are an infinite number of solutions of the given equation, one for each value of t.

Example 2.4. Consider the linear Diophantine equation

$$172x + 20y = 1000$$

Applying the Euclidean's Algorithm to the evaluation of gcd(172, 20), we find that

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

whence $\gcd(172, 20) = 4$. Because $4 \mid 1000$, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \\ &= 2 \cdot 172 + (-17)20 \end{aligned}$$

Upon multiplying this relation by 250, we arrive at

$$\begin{aligned} 1000 = 250 \cdot 4 &= 250[2 \cdot 172 + (-17)20] \\ &= 500 \cdot 172 + (-4250)20 \end{aligned}$$

so that $x = 500$ and $y = -4250$ provide one solution to the Diophantine equation in question. All other solutions are expressed by

$$\begin{aligned} x &= 500 + (20/4)t = 500 + 5t \\ y &= -4250 - (172/4)t = -4250 - 43t \end{aligned}$$

for some integer t.

A little further effort produces the solutions in the positive integers, if any happen to exist. For this, t must be chosen to satisfy simultaneously the inequalities

$$5t + 500 > 0 \qquad -43t - 4250 > 0$$

or, what amounts to the same thing,

$$-98\frac{36}{43} > t > -100$$

Because t must be an integer, we are forced to conclude that $t = -99$. Thus, our Diophantine equation has a unique positive solution $x = 5$, $y = 7$ corresponding to the value $t = -99$.

It might be helpful to record the form that Theorem 2.9 takes when the coefficients are relatively prime integers.

Corollary. If $\gcd(a, b) = 1$ and if x_0, y_0 is a particular solution of the linear Diophantine equation $ax + by = c$, then all solutions are given by

$$x = x_0 + bt \qquad y = y_0 - at$$

for integral values of t.

Here is an example. The equation $5x + 22y = 18$ has $x_0 = 8$, $y_0 = -1$ as one solution; from the corollary, a complete solution is given by $x = 8 + 22t$, $y = -1 - 5t$ for arbitrary t.

Diophantine equations frequently arise when solving certain types of traditional word problems, as evidenced by Example 2.5.

Example 2.5. A customer bought a dozen pieces of fruit, apples and oranges, for \$1.32. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

To set up this problem as a Diophantine equation, let x be the number of apples and y be the number of oranges purchased; in addition, let z represent the cost (in cents) of an orange. Then the conditions of the problem lead to

$$(z + 3)x + zy = 132$$

or equivalently

$$3x + (x + y)z = 132$$

Because $x + y = 12$, the previous equation may be replaced by

$$3x + 12z = 132$$

which, in turn, simplifies to $x + 4z = 44$.

Stripped of inessentials, the object is to find integers x and z satisfying the Diophantine equation

$$x + 4z = 44 \tag{1}$$

Inasmuch as $\gcd(1, 4) = 1$ is a divisor of 44, there is a solution to this equation. Upon multiplying the relation $1 = 1(-3) + 4 \cdot 1$ by 44 to get

$$44 = 1(-132) + 4 \cdot 44$$

it follows that $x_0 = -132$, $z_0 = 44$ serves as one solution. All other solutions of Eq. (1) are of the form

$$x = -132 + 4t \qquad z = 44 - t$$

where t is an integer.

Not all of the choices for t furnish solutions to the original problem. Only values of t that ensure $12 \geq x > 6$ should be considered. This requires obtaining those values of t such that

$$12 \geq -132 + 4t > 6$$

Now, $12 \geq -132 + 4t$ implies that $t \leq 36$, whereas $-132 + 4t > 6$ gives $t > 34\frac{1}{2}$. The only integral values of t to satisfy both inequalities are $t = 35$ and $t = 36$. Thus, there are two possible purchases: a dozen apples costing 11 cents apiece (the case where $t = 36$), or 8 apples at 12 cents each and 4 oranges at 9 cents each (the case where $t = 35$).

Linear indeterminate problems such as these have a long history, occurring as early as the 1st century in the Chinese mathematical literature. Owing to a lack of algebraic symbolism, they often appeared in the guise of rhetorical puzzles or riddles.

The contents of the *Mathematical Classic* of Chang Ch′ iu-chien (6th century) attest to the algebraic abilities of the Chinese scholars. This elaborate treatise contains one of the most famous problems in indeterminate equations, in the sense of transmission to other societies—the problem of the "hundred fowls." The problem states:

> If a cock is worth 5 coins, a hen 3 coins, and three chicks together 1 coin, how many cocks, hens, and chicks, totaling 100, can be bought for 100 coins?

In terms of equations, the problem would be written (if x equals the number of cocks, y the number of hens, z the number of chicks):

$$5x + 3y + \frac{1}{3}z = 100 \qquad x + y + z = 100$$

Eliminating one of the unknowns, we are left with a linear Diophantine equation in the two other unknowns. Specifically, because the quantity $z = 100 - x - y$, we have $5x + 3y + \frac{1}{3}(100 - x - y) = 100$, or

$$7x + 4y = 100$$

This equation has the general solution $x = 4t$, $y = 25 - 7t$, so that $z = 75 + 3t$, where t is an arbitrary integer. Chang himself gave several answers:

$$\begin{array}{lll} x = 4 & y = 18 & z = 78 \\ x = 8 & y = 11 & z = 81 \\ x = 12 & y = 4 & z = 84 \end{array}$$

A little further effort produces all solutions in the positive integers. For this, t must be chosen to satisfy simultaneously the inequalities

$$4t > 0 \qquad 25 - 7t > 0 \qquad 75 + 3t > 0$$

The last two of these are equivalent to the requirement $-25 < t < 3\frac{4}{7}$. Because t must have a positive value, we conclude that $t = 1, 2, 3$, leading to precisely the values Chang obtained.

PROBLEMS 2.5

1. Which of the following Diophantine equations cannot be solved?
   (a) $6x + 51y = 22$.
   (b) $33x + 14y = 115$.
   (c) $14x + 35y = 93$.

2. Determine all solutions in the integers of the following Diophantine equations:
   (a) $56x + 72y = 40$.
   (b) $24x + 138y = 18$.
   (c) $221x + 35y = 11$.

3. Determine all solutions in the positive integers of the following Diophantine equations:
   (a) $18x + 5y = 48$.
   (b) $54x + 21y = 906$.
   (c) $123x + 360y = 99$.
   (d) $158x - 57y = 7$.

4. If a and b are relatively prime positive integers, prove that the Diophantine equation $ax - by = c$ has infinitely many solutions in the positive integers.
[*Hint:* There exist integers x_0 and y_0 such that $ax_0 + by_0 = c$. For any integer t, which is larger than both $|x_0|/b$ and $|y_0|/a$, a positive solution of the given equation is $x = x_0 + bt$, $y = -(y_0 - at)$.]

5. (a) A man has \$4.55 in change composed entirely of dimes and quarters. What are the maximum and minimum number of coins that he can have? Is it possible for the number of dimes to equal the number of quarters?
(b) The neighborhood theater charges \$1.80 for adult admissions and \$.75 for children. On a particular evening the total receipts were \$90. Assuming that more adults than children were present, how many people attended?
(c) A certain number of sixes and nines is added to give a sum of 126; if the number of sixes and nines is interchanged, the new sum is 114. How many of each were there originally?

6. A farmer purchased 100 head of livestock for a total cost of \$4000. Prices were as follow: calves, \$120 each; lambs, \$50 each; piglets, \$25 each. If the farmer obtained at least one animal of each type, how many of each did he buy?

7. When Mr. Smith cashed a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa. Unaware of this, Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written.
[*Hint:* If x denotes the number of dollars and y the number of cents in the check, then $100y + x - 68 = 2(100x + y)$.]

8. Solve each of the puzzle-problems below:
(a) Alcuin of York, 775. One hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman 2 bushels, and each child $\frac{1}{2}$ bushel. How many men, women, and children are there?
(b) Mahaviracarya, 850. There were 63 equal piles of plantain fruit put together and 7 single fruits. They were divided evenly among 23 travelers. What is the number of fruits in each pile?
[*Hint:* Consider the Diophantine equation $63x + 7 = 23y$.]
(c) Yen Kung, 1372. We have an unknown number of coins. If you make 77 strings of them, you are 50 coins short; but if you make 78 strings, it is exact. How many coins are there?
[*Hint:* If N is the number of coins, then $N = 77x + 27 = 78y$ for integers x and y.]
(d) Christoff Rudolff, 1526. Find the number of men, women, and children in a company of 20 persons if together they pay 20 coins, each man paying 3, each woman 2, and each child $\frac{1}{2}$.
(e) Euler, 1770. Divide 100 into two summands such that one is divisible by 7 and the other by 11.