CHAPTER 2

THE FUNDAMENTAL THEOREM OF ARITHMETIC

In every branch of mathematics we meet theorems that seem so natural that, if we held no respect for logical rigor, we would be tempted to take them for granted. We must prove such theorems carefully, not only because they may be crucial in the logical structure of the theory, but also because every few years some proposition whose denial has long appeared to be utterly unacceptable to common sense turns out to be false.

You are now acquainted with one of these important theorems, the basis representation theorem (Theorem 1–3). This chapter will culminate in another basic proposition, the fundamental theorem of arithmetic (Theorem 2–5), from which we shall obtain significant information about the multiplicative structure of the integers. In passing, we note that a certain apparently obvious extension of the theorem to other number-theoretic structures resembling the integers is false (see Exercise 1 in Section 2–4).

We begin by developing Euclid's division lemma (Theorem 2–1), by means of which we shall study the divisibility properties of integers (Theorems 2–2 and 2–3). Knowledge of these properties will enable us to prove the fundamental theorem of arithmetic.

2–1 EUCLID'S DIVISION LEMMA

The division lemma furnishes the foundation for much of number theory; yet it is simply a rigorous restatement of the well-known fact that division of one integer by another yields an integral quotient and an integral nonnegative remainder smaller than the divisor. In order to avoid unnecessary complications, we limit ourselves to positive divisors. The proof we shall give for the lemma relies heavily on the basis representation theorem.

THEOREM 2–1 *(Euclid's Division Lemma): For any integers k $(k > 0)$ and j, there exist unique integers q and r such that $0 \le r < k$ and*

remember: $q = \lfloor j/k \rfloor$ = quotient

$$j = qk + r. \tag{2-1-1}$$

r = remainder = $j - qk$

PROOF: Note that we have simply rewritten a division problem in terms of multiplication and addition. In the notation used above, j is the dividend; k, the divisor; q, the quotient; and r, the remainder.

If $k = 1$, r must be zero, so that $q = j$.

If $k > 1$, suppose first that $j > 0$. (We shall consider the cases in which $j = 0$ and $j < 0$ later.) By the basis representation theorem (Theorem 1–3), j has a unique representation to the base k, say

$$\begin{aligned} j &= a_s k^s + a_{s-1}k^{s-1} + \dots + a_1 k + a_0 \\ &= k(a_s k^{s-1} + a_{s-1}k^{s-2} + \dots + a_1) + a_0 \\ &= kq + r, \end{aligned}$$

where $0 \le r = a_0 < k$.

If a second pair q' and r' existed, we could find a representation for q' to the base k, say

$$q' = b_t k^t + \dots + b_1 k + b_0,$$

so that

$$\begin{aligned} j &= kq' + r' \\ &= b_t k^{t+1} + \dots + b_1 k^2 + b_0 k + r', \end{aligned}$$

but

$$j = a_s k^s + a_{s-1}k^{s-1} + \dots + a_1 k + a_0.$$

By the uniqueness of the representation of j to the base k, we see that $t = s - 1$, $b_i = a_{i+1}$, $r' = a_0 = r$, and thus

$$\begin{aligned} q' &= b_t k^t + \dots + b_1 k + b_0 \\ &= a_s k^{s-1} + \dots + a_2 k + a_1 \\ &= q. \end{aligned}$$

Consequently, the theorem is true for positive values of j.

If $j = 0$, it is easy to verify that $q = r = 0$ is the only possible solution of (2–1–1) with $0 \le r < k$.

If $j < 0$, then $-j > 0$, and there exist unique integers q'' and r'' such that

$$-j = kq'' + r''.$$

If $r'' = 0$, then $j = k(-q'')$; thus we may take $q = -q''$ and $r = 0$. If $r'' \neq 0$, then

$$\begin{aligned} j &= -kq'' - r'' \\ &= k(-q'' - 1) + (k - r''), \end{aligned}$$

and we may take $q = -q'' - 1$, and $r = k - r''$.

In either case, q and r satisfy equation (2–1–1). Uniqueness for negative j follows from uniqueness for $-j$, which is then positive. ■

EXERCISES

1. Without assuming Theorem 2–1, prove that for each pair of integers j and $k (k > 0)$, there exists some integer q for which $j - qk$ is positive.

2. The principle of mathematical induction is equivalent to the following statement, called the least-integer principle: *Every non-empty set of positive integers has a least element.*

   Using the least integer principle, define r to be the least integer for which $j - qk$ is positive (see Exercise 1). Prove that $0 < r \leq k$.

3. Use Exercise 2 to give a new proof of Theorem 2–1.

4. Any nonempty set of integers J that fulfills the following two conditions is called an *integral ideal:*

   (i) if n and m are in J, then $n + m$ and $n - m$ are in J; and
   (ii) if n is in J and r is an integer, then rn is in J.

   Let $\mathscr{I}_m$ be the set of all integers that are integral multiples of a particular integer m. Prove that $\mathscr{I}_m$ is an integral ideal.

5. Prove that every integral ideal J is identical with $\mathscr{I}_m$ for some m. [Hint: Prove that if $J \neq \{0\} = \mathscr{I}_0$, then there exist positive integers in J. By the least-integer principle (Exercise 2), there is a least positive integer in J, say m. Then prove that $J = \mathscr{I}_m$.]

6. Prove that if a and b are odd integers, then $a^2 - b^2$ is divisible by 8.

7. Prove that if a is an odd integer, then $\{a^2 + (a+2)^2 + (a+4)^2 + 1\}$ is divisible by 12.

2–2 DIVISIBILITY

If a and $b (b \neq 0)$ are integers, we say *b divides a*, or *b is a divisor of a*, if a/b is an integer. We shall write $b \mid a$ to indicate that b divides a; and, $b \nmid a$, to indicate that b does not divide a.

Example 2–1: $2 \mid 4$, but $3 \nmid 4$.

Example 2–2: If a is an integer, then $1 \mid a$ and $-1 \mid a$; furthermore, if $a \neq 0$, then $a \mid a$ and $-a \mid a$.

Example 2–3: For each nonzero integer a, $a \mid 0$.

Example 2–4: Let a, b, c, and d be integers. Suppose that an integer e divides both a and c. Then there exist integers x and y such that $a = ex$ and $c = ey$. Therefore,

$$\begin{aligned} ab + cd &= exb + eyd \\ &= e(xb + yd), \end{aligned}$$

which implies that $e \mid (ab + cd)$. Consequently, if $e \mid a$ and $e \mid c$, then $e \mid (ab + cd)$ also.

If a and b are integers, then any integer that divides both a and b is called a *common divisor* of a and b.

Definition 2–1: *If a and b are integers, not both zero, then an integer d is called the* **greatest common divisor** *of a and b if*

(i) $d > 0$,
(ii) *d is a common divisor of a and b, and*
(iii) *each integer f that is a common divisor of both a and b is also a divisor of d.*

We shall prove shortly that each pair of integers a and b, not both zero, has a unique greatest common divisor; this integer is denoted by g.c.d.(a,b). Many authors write (a,b) for g.c.d.(a,b). We do not, because we shall often use (a,b) to represent a point in the Euclidean plane.

Example 2–5: The positive divisors of 12 are 1, 2, 3, 4, 6, and 12. The positive divisors of -8 are 1, 2, 4, and 8. Thus the positive common divisors of 12 and -8 are 1, 2, and 4; hence, g.c.d.$(12,-8) = 4$.

Example 2–6: If $a \neq 0$ and $a \mid b$, then g.c.d.$(a,b) = |a|$.

Our proof of the existence and uniqueness of the greatest common divisor depends completely on the Euclidean algorithm, a device involving nothing more than repeated application of the division lemma. Before proceeding with the proof, we illustrate the Euclidean algorithm with the following example.

Example 2–7: What is g.c.d.(341,527)? Dividing 341 into 527, we find that the q and r, as in Theorem 2–1, are 1 and 186, respectively, because

$$527 = 341 \cdot 1 + 186 \qquad \text{(2-2-2)}$$

Clearly, any number that divides both 527 and 341 also divides 186; for, if $dc = 527$ and $de = 341$, then $d(c-e) = 186$.

In the same manner,

$$341 = 186 \cdot 1 + 155, \qquad \text{(2-2-3)}$$

$$186 = 155 \cdot 1 + 31, \text{ and} \qquad \text{(2-2-4)}$$

$$155 = 31 \cdot 5. \qquad \text{(2-2-5)}$$

By equation (2–2–5), 31 divides 155. Therefore 31 divides 186, by (2–2–4); $31 \mid 341$, by (2–2–3); and $31 \mid 527$, by (2–2–2). Thus 31 satisfies (i) and (ii) in Definition 2–1. Finally, if $f \mid 341$ and $f \mid 527$, then $f \mid 186$, by (2–2–2); $f \mid 155$, by (2–2–3); and $f \mid 31$, by (2–2–4). Since all three conditions in Definition 2–1 are satisfied, we see that $31 =$ g.c.d.(341,527).

The proof of Theorem 2 involves nothing more than the procedure of Example 2–7 in a general setting.

Theorem 2–2: *If a and b are integers, not both zero, then g.c.d.(a,b) exists and is unique.*

Proof: Clearly g.c.d.(a,b) is not affected by the signs of a and b. We have asserted that not both a and b are zero; however, if either is zero, say $b = 0$, then g.c.d.$(a,0)$ is clearly equal to $|a|$. In the following proof, we may therefore assume that $a \geq b > 0$.

By Theorem 2–1, there exist q_1 and r_1 $(0 \leq r_1 < b)$ such that

$$a = bq_1 + r_1.$$

If $r_1 > 0$, there exist q_2 and r_2 such that

$$b = r_1 q_2 + r_2,$$

where $0 \leq r_2 < r_1$. If $r_2 > 0$, there exist q_3 and r_3 such that

$$r_1 = r_2 q_3 + r_3,$$

where $0 \leq r_3 < r_2$. This process may be continued as long as the newly arising r_i does not equal zero.

Since

$$b > r_1 > r_2 > r_3 > \ldots > 0,$$

we see, by mathematical induction, that $0 \leq r_i \leq b - i$. Therefore, in at most b steps, we shall obtain an r_n that is zero.

Thus the last application of Theorem 2–1 in our procedure leads to the result

$$r_{n-2} = r_{n-1} q_n + 0;$$

that is, $r_n = 0$. The computation of g.c.d.(341,527) in Example 2–7 suggests that r_{n-1} is equal to g.c.d.(a,b).

We have constructed the r_i so that $r_{n-1} > 0$. By working backward from the final equation, we may establish successively that r_{n-1} divides $r_{n-2}, r_{n-3}, \ldots, r_2, r_1, b$, and a. Finally, if f divides both a and b, we may proceed successively from the initial equation to deduce that f divides $r_1, r_2, \ldots, r_{n-2}$, and r_{n-1}. (Mathematical induction is tacitly used in both of these procedures.) Thus r_{n-1} satisfies the requirements of Definition 2–1; therefore, $r_{n-1} =$ g.c.d.(a,b).

Each pair of integers has only one greatest common divisor; for, if both d_1 and d_2 are greatest common divisors of some pair a and b, it follows from (iii) of Definition 2–1 that $gd_1 = d_2$ and $hd_2 = d_1$, where h and g are positive integers; hence, $d_2 = ghd_2$; thus $1 = gh$, and so $g = h = 1$. We conclude that $d_1 = d_2$. ■

An *integral linear combination* of the integers a and b is an expression of the form $ax + by$, where x and y are integers. We shall prove two corollaries of Theorem 2–2 that characterize those integers expressible as integral linear combinations of a particular pair of integers. First we consider an example.

Example 2–8: Using the results in Example 2–7, we shall express $31 = \text{g.c.d.}(341,527)$ as an integral linear combination of 341 and 527. We start with the next-to-the-last equation and successively substitute the other equations into it until we reach the initial equation. Equation (2–2–3) may be rewritten as

$$31 = 186 - 155 \cdot 1.$$

Using equation (2–2–3) to express 155, we find that

$$31 = 186 - (341 - 186 \cdot 1),$$

that is,

$$31 = 2 \cdot 186 - 341.$$

Using equation (2–2–2) to express 186, we see that

$$31 = 2 \cdot (527 - 341 \cdot 1) - 341,$$

that is,

$$31 = 2 \cdot 527 - 3 \cdot 341.$$

Thus we have expressed 31 as a linear combination of 341 and 527.

Note that, in addition,

$$31 = 14 \cdot 341 - 9 \cdot 527,$$

and

$$31 = -20 \cdot 341 + 13 \cdot 527.$$

In general, there may be many pairs x and y such that

$$\text{g.c.d.}(a,b) = ax + by.$$

Corollary 2–1: *If $d = \text{g.c.d.}(a,b)$, then there exist integers x and y such that*

$$ax + by = d. \qquad (2\text{-}2\text{-}6)$$

Proof: By taking the n equations used in the proof of Theorem 2–2 and using the principle of mathematical induction, we shall first establish that there exist integers x_i and y_i such that

$$ax_i + by_i = r_i \qquad (2\text{-}2\text{-}7)$$

for $i = 1, 2, \ldots, n-1$.

When $i = 1$, let $x_1 = 1$, and $y_1 = -q_1$. Now assume that integer solutions of (2–2–7) have been found for all i less than or equal to $k(k < n-1)$. We know that

$$r_{k-1} = r_k q_{k+1} + r_{k+1}; \qquad (2\text{-}2\text{-}8)$$

thus, by the induction hypothesis,

$$(ax_{k-1} + by_{k-1}) - (ax_k + by_k)q_{k+1} = r_{k+1}. \qquad (2\text{-}2\text{-}9)$$

We can rewrite equation (2–2–9) in the form

$$(x_{k-1} - x_k q_{k+1})a + (y_{k-1} - y_k q_{k-1})b = r_{k+1}. \qquad (2\text{-}2\text{-}10)$$

Hence, $x_{k+1} = x_{k-1} - x_k q_{k+1}$ and $y_{k+1} = y_{k-1} - y_k q_{k-1}$ are solutions of equation (2–2–7) when $i = k+1$.

Thus formula (2–2–7) is established for $i = 1, 2, \ldots, n-1$, by the principle of mathematical induction. In particular, if $i = n-1$ in equation (2–2–7), we get the relation

$$ax_{n-1} + by_{n-1} = r_{n-1} = \text{g.c.d.}(a,b). \qquad ■$$

Corollary 2–2: *In order that there exist integers x and y satisfying the equation*

A⇐⇒B

$$ax + by = c, \qquad (2\text{-}2\text{-}11)$$

it is necessary and sufficient that $d \mid c$, where $d = \text{g.c.d.}(a,b)$.

Proof: Let $a = ed$, $b = fd$. Then, if (2–2–11) holds, we get the relation

A⇒B

$$c = edx + fdy = d(ex + fy).$$

Thus $d \mid c$.

On the other hand, if $d \mid c$, let $kd = c$. Then, by Corollary 2–1,

B⇒A

there exist x' and y' such that

$$ax' + by' = d.$$

Hence

$$a(x'k) + b(y'k) = dk = c.$$

Thus $x = x'k$ and $y = y'k$ provide a solution of (2–2–11). ■

Our next theorem follows from Corollary 2–2; it will be the principal tool we shall use in our proof of the fundamental theorem of arithmetic. First we need some further definitions.

DEFINITION 2–2: *A positive integer p other than 1 is said to be* **a prime** *if its only positive divisors are* 1 and p.

The first few primes are 2, 3, 5, 7, 11, ... (Although the 1968 World Almanac lists 1 as a prime, it is convenient not to do so in number theory. As you will see, the statement of the fundamental theorem of arithmetic would be needlessly complicated if 1 were considered prime. Perhaps this fact has been impressed on the editors of the Almanac, for the 1969 and later editions do not list 1 as a prime.) The primes have many interesting properties, some of which we shall explore in later sections.

DEFINITION 2–3: *We say that a and b are* **relatively prime** *if* g.c.d.$(a,b) = 1$.

Example 2–9: The positive divisors of 7 are 1 and 7. The positive divisors of 27 are 1, 3, 9, and 27. Since 1 is the only positive common divisor of 7 and 27, these two integers are relatively prime.

Example 2–10: If $d =$ g.c.d.(a,b), then a/d and b/d are relatively prime. To show this, let x and y be integers such that $ax + by = d$. Then $(a/d)x + (b/d)y = 1$, and so g.c.d.$(a/d, b/d) = 1$.

Example 2–11: If p is a prime and a is an integer such that $p \nmid a$, then p and a are relatively prime. In particular, any two different primes are relatively prime.

THEOREM 2–3: *If a, b, and c are integers, where a and c are relatively prime, and if $c \mid ab$, then c divides b.*

PROOF: Since g.c.d.$(a,c) = 1$, Corollary 2–2 implies that there exist integers x and y such that

$$cx + ay = 1.$$

Therefore,

$$cbx + aby = b. \qquad (2\text{-}2\text{-}12)$$

Since $c \mid ab$, there exists a k such that $ab = kc$.

Substituting kc for ab in equation (2–2–12), we find that

$$cbx + kcy = b. \qquad (2\text{-}2\text{-}13)$$

Thus

$$c(bx + ky) = b. \qquad (2\text{-}2\text{-}14)$$

Hence $c \mid b$. ■

COROLLARY 2–3: *If a and b are integers, p is a prime, $p \mid ab$, and $p \nmid a$, then $p \mid b$.*

PROOF: If $p \nmid a$, then g.c.d.$(a,p) = 1$, because the only positive divisors of p are 1 and p. Hence, by Theorem 2–3 (with $c = p$), we see that $p \mid b$. ■

COROLLARY 2–4: *If $p \mid a_1a_2 \ldots a_n$, then there exists some i such that $p \mid a_i$.*

PROOF: We proceed by mathematical induction. The assertion is clear for $n = 1$. For $n = 2$, it is a restatement of Corollary 2–3. We assume that the assertion is true for n less than or equal to k. Then for $n = k + 1$ we consider the relation

$$p \mid (a_1a_2 \ldots a_k)a_{k+1}.$$

By Corollary 2–3, either $p \mid a_{k+1}$ (so that $i = k + 1$) or $p \mid a_1a_2 \ldots a_k$, in which case $p \mid a_i$ for some $i(1 \leq i \leq k)$, by the induction hypothesis. ■

EXERCISES

1. Using the technique described in Example 2–7, find the greatest common divisor of the following pairs of integers.

(a) 527, 765 (d) 108, 243

(b) 361, 1178 (e) 132, 473

(c) 12321, 8658 (f) 156, 1740.

2. Using the technique described in Example 2–8, find the greatest common divisor d of 299 and 481. Then find integers x and y such that

$$299x + 481y = d.$$

3. In Exercise 2, replace 299 and 481 by 129 and 301 and proceed as indicated.

4. The *least common multiple* of two positive integers a and b (denoted by l.c.m.(a,b)) is defined to be the smallest positive integer that is divisible by both a and b. Prove that

$$\text{l.c.m.}(a,b) = \frac{ab}{\text{g.c.d.}(a,b)}.$$

5. Compute the following:

(a) l.c.m.(25,30) (d) l.c.m.(28,29)

(b) l.c.m.(42,49) (e) l.c.m.$(n,n+1)$

(c) l.c.m.(27,81) (f) l.c.m.$(2n-1,2n+1)$.

6. Prove that l.c.m.$(ab,ad) = a[\text{l.c.m.}(b,d)]$.

7. Prove that if $D = d/\text{g.c.d.}(b,d)$ and $B = b/\text{g.c.d.}(b,d)$, then

$$\frac{a}{b} + \frac{c}{d} = \frac{aD + cB}{\text{l.c.m.}(b,d)}.$$

Discuss the relationship between this equation and the addition of fractions by means of a "common denominator".

8. Prove that g.c.d.$(a+b, a-b) \geq$ g.c.d.(a,b).

9. Prove that, if a and b are nonzero integers, then g.c.d.$(a,b) \mid$ l.c.m.(a,b).

10. Let $\mathscr{I}_m$ be the set of all integral multiples of the integer m. Prove that

$$\mathscr{I}_m \cap \mathscr{I}_n = \mathscr{I}_{\text{l.c.m.}(m,n)}.$$

[If S and T are sets, then $S \cap T$ denotes the set of elements common to both S and T].

11. Prove that $\mathscr{I}_{\text{g.c.d.}(m,n)}$ contains all the elements of $\mathscr{I}_m$ and all the elements of $\mathscr{I}_n$. Prove that if $\mathscr{I}_r$ contains all the elements of $\mathscr{I}_m$ and $\mathscr{I}_n$, then $\mathscr{I}_r$ contains all the elements of $\mathscr{I}_{\text{g.c.d.}(m,n)}$.

12. We can define a *generalized Fibonacci sequence* $\mathscr{F}_1, \mathscr{F}_2, \mathscr{F}_3, \mathscr{F}_4, \ldots$ by first selecting four integers a, b, c, and e, and then letting $\mathscr{F}_1 = a$, $\mathscr{F}_2 = b$, and $\mathscr{F}_n = c\mathscr{F}_{n-1} + e\mathscr{F}_{n-2}$ if $n > 2$.

(a) Prove that, if $d = \text{g.c.d.}(a,b)$, then $d \mid \mathscr{F}_n$ for all $n \geq 1$.

(b) Prove that, if $f = \text{g.c.d.}(\mathscr{F}_m, \mathscr{F}_{m-1})$ and g.c.d.$(f,e) = 1$, then $f \mid d$.

2–3 THE LINEAR DIOPHANTINE EQUATION

We have now amassed enough results to prove the fundamental theorem of arithmetic. Before beginning this task, however, we shall consider a result related to Corollary 2–2.

Let a, b, and c be integers ($a \neq 0 \neq b$). The expression

$$ax + by = c \tag{2-3-1}$$

is called a *linear Diophantine equation.* A *solution* of this equation is a pair (x,y) of integers that satisfies the equation.

From analytic geometry we know that each point in a plane can be associated with an ordered pair of real numbers called coordinates. A point whose coordinates are integers is called a *lattice point.* In the plane, the locus of points whose coordinates x and y satisfy equation (2–3–1) is a straight line. Thus the solutions of this linear Diophantine equation correspond to the lattice points lying on the straight line. Depending on the values of a, b, and c, there may be none or many lattice points on the graph of $ax + by = c$.

From Corollary 2–2 we know that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \text{g.c.d.}(a,b)$. Suppose that d *does* divide c. Using the procedure illustrated in Example 2–8, we can find w_0 and z_0 such that

$$aw_0 + bz_0 = d.$$

Next, we find an integer k such that $c = dk$; and we let $x_0 = w_0k$ and $y_0 = z_0k$. Clearly, (x_0,y_0) is a solution of equation (2–3–1). Suppose (x',y') is also a solution of equation (2–3–1). Then

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

and so

$$\frac{a}{d}x' + \frac{b}{d}y' = \frac{a}{d}x_0 + \frac{b}{d}y_0.$$

Therefore,

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y'). \tag{2-3-2}$$

By Example 2–10, g.c.d.$(a/d, b/d) = 1$; thus, by Theorem 2–3,

$$\frac{b}{d} \,\Big|\, (x' - x_0).$$

Hence, there exists an integer t such that $x' - x_0 = tb/d$; that is, $x' = x_0 + tb/d$. Substituting tb/d for $x' - x_0$ in equation (2–3–2), we find that

$$\frac{a}{d}t\frac{b}{d} = \frac{b}{d}(y_0 - y'),$$

and so

$$y_0 - y' = t\frac{a}{d},$$

that is,

$$y' = y_0 - t\frac{a}{d}.$$

We conclude that, for each solution (x', y') of equation (2–3–1), there exists an integer t such that

$$x' = x_0 + t\frac{b}{d} \quad \text{and} \quad y' = y_0 - t\frac{a}{d}.$$

In fact, $(x_0 + tb/d,\ y_0 - ta/d)$ is a solution of equation (2–3–1) for each t, because

$$a\left(x_0 + t\frac{b}{d}\right) + b\left(y_0 - t\frac{a}{d}\right) = ax_0 + by_0 + t\frac{ab}{d} - t\frac{ab}{d} = c.$$

We now summarize the preceding results.

Theorem 2–4: *The linear Diophantine equation*

$$ax + by = c$$

has a solution if and only if $d \mid c$, where $d =$ g.c.d.(a,b). Furthermore, if (x_0, y_0) is a solution of this equation, then the set of solutions of the equation consists of all integer pairs (x,y), where

$$x = x_0 + t\frac{b}{d} \quad \textit{and} \quad y = y_0 - t\frac{a}{d} \qquad (t = \ldots, -2, -1, 0, 1, 2, \ldots).$$

Example 2–12: The linear Diophantine equation $15x + 27y = 1$ has no solutions, since g.c.d.$(15,27) = 3$ and $3 \nmid 1$.

Example 2–13: The linear Diophantine equation $5x + 6y = 1$ has a solution, since g.c.d.$(5,6) = 1$. By inspection, we see that $(-1, 1)$ is such a solution. Hence, all solutions are given by (x,y), where $x = -1 + 6t$, $y = 1 - 5t$ $(t = \ldots -2, -1, 0, 1, 2, \ldots)$.

EXERCISES

1. Find the general solution (if solutions exist) of each of the following linear Diophantine equations:
   (a) $2x + 3y = 4$ (d) $23x + 29y = 25$
   (b) $17x + 19y = 23$ (e) $10x - 8y = 42$
   (c) $15x + 51y = 41$ (f) $121x - 88y = 572$.
2. A man pays \$1.43 for some apples and pears. If pears cost 17¢ each, and apples, 15¢ each, how many of each did he buy?
3. Draw the graphs of the straight lines defined by the equations in parts (a), (b), and (c) of Exercise 1.
4. Prove that the area of the triangle whose vertices are $(0,0)$, (b,a), and (x,y) is $|by - ax|/2$.
5. Prove that if (x_0, y_0) is a solution of the linear Diophantine equation $ax - by = 1$, then the area of the triangle whose vertices are $(0,0)$, (b,a), and (x_0, y_0) is 1/2.
6. Is there a nondegenerate triangle with area smaller than 1/2 and with vertices (p_1, q_1), (p_2, q_2), and (p_3, q_3), where the p_i and q_i are integers? Prove your answer.
7. What is the perpendicular distance to the origin (0,0) from the line defined by the equation

$$ax - by = 1?$$

8. What is the shortest possible distance between two lattice points on the line defined by the linear Diophantine equation

$$ax - by = c?$$

(Recall that, by the definition of a linear Diophantine equation, the constants a, b, and c must be integers.)

2–4 THE FUNDAMENTAL THEOREM OF ARITHMETIC

Table 2–1 exhibits the ways the first twelve positive integers may be factored into primes.

The evidence of Table 2–1 suggests that there is exactly one prime factorization of each integer greater than 1, if the order of the prime factors is disregarded.

While not as intuitively apparent as the basis representation theorem (Theorem 1–3), the foregoing conjecture not only is true, but is so important to the study of integers that it is called the fundamental theorem of arithmetic.

Theorem 2–5 *(Fundamental Theorem of Arithmetic): For each integer $n > 1$, there exist primes $p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_r$ such that*

$$n = p_1 p_2 \ldots p_r;$$

this factorization is unique.

Proof: Our first goal is to prove that each integer has at least one prime factorization. Note that (see Table 2–1) such a factorization

Table 2–1: Factorization of Integers Into Primes.

n	factorizations
1	–
2	2
3	3
4	$2 \cdot 2$
5	5
6	$2 \cdot 3 = 3 \cdot 2$
7	7
8	$2 \cdot 2 \cdot 2$
9	$3 \cdot 3$
10	$2 \cdot 5 = 5 \cdot 2$
11	11
12	$2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$

exists for all $n (2 \leq n \leq 12)$. Let us now assume that each integer $m (1 < m \leq k)$ can be factored into primes.

Now, either $k + 1$ is prime or it is not. If it is prime, then its prime factorization consists just of the prime itself. If $k + 1$ is not prime, then

$$k + 1 = ab,$$

where $1 < a < k + 1$ and $1 < b < k + 1$. Since $1 < a \leq k$ and $1 < b \leq k$, both a and b have prime factorizations, say

$$a = p_1 p_2 \ldots p_s \quad \text{and} \quad b = p_1' p_2' \ldots p_t'.$$

Therefore,

$$k + 1 = p_1 p_2 \ldots p_s p_1' p_2' \ldots p_t'.$$

Hence $k + 1$ has a prime factorization. Thus we have established by mathematical induction that every integer greater than 1 has a prime factorization.

To complete the theorem, we must establish uniqueness of factorization. Again we proceed by mathematical induction. Our table also tells us that the factorization of each n ($n \leq 12$) is unique. Assume that each integer $m (1 < m \leq k)$ has a unique prime factorization. Suppose that $k + 1$ has the two prime factorizations

$$k + 1 = p_1 p_2 \ldots p_u = p_1' p_2' \ldots p_v',$$

where $p_1 \leq p_2 \leq \ldots \leq p_u$ and $p_1' \leq p_2' \leq \ldots \leq p_v'$. Since p_1' divides $k + 1$, we see that p_1' divides $p_1 p_2 \ldots p_u$; thus p_1' divides p_i for some i, by Corollary 2–4. Since both p_1' and p_i are primes, we conclude that $p_1' = p_i$.

Clearly, we may reverse the preceding argument to show that $p_1 = p_j'$ for some j. Hence

$$p_1 = p_j' \geq p_1',$$

and

$$p_1' = p_i \geq p_1.$$

Therefore, $p_1 \geq p_1' \geq p_1$; and so $p_1 = p_1'$. Thus $(k+1)/p_1$ is an integer not exceeding k, and

$$p_2 \ldots p_u = \frac{k+1}{p_1} = p_2' \ldots p_v'.$$

Hence, by the induction hypothesis, $u = v$, $p_2' = p_2, \ldots$, and $p_u' = p_u$. Thus the fundamental theorem of arithmetic is established. ■

EXERCISES

1. Let E be the set of all positive even integers. Define m to be an "even prime" if m is even but is not factorable into two even numbers. Prove that some elements of E are not uniquely representable as products of even primes.

2. Prove that every positive integer is uniquely representable as the product of a nonnegative power of 2 (perhaps 2^0) and an odd number.

3. Suppose that $a = p_1p_2 \ldots p_s$ is the unique factorization of a into primes ($p_1 \leq p_2 \leq \ldots \leq p_s$). Prove that a has a unique representation

$$q_1^{e_1}q_2^{e_2} \ldots q_r^{e_r},$$

where the q_i are primes, $q_1 < q_2 < \ldots < q_r$, and the e_i are positive integers.

4. Prove that, if $a = q_1^{e_1}q_2^{e_2} \ldots q_r^{e_r}$ and $b = s_1^{f_1}s_2^{f_2} \ldots s_u^{f_u}$ are the factorizations of a and b into primes (see Exercise 3), then there exist primes $t_1 < t_2 < \ldots < t_v$ and nonnegative integers g_i and h_i such that

$$a = t_1^{g_1}t_2^{g_2} \ldots t_v^{g_v}, \text{ and } b = t_1^{h_1}t_2^{h_2} \ldots t_v^{h_v}.$$

5. Using the notation of Exercise 4, prove that

$$\text{g.c.d.}(a,b) = t_1^{c_1}t_2^{c_2} \ldots t_v^{c_v},$$

where each c_i is the smaller of the corresponding g_i and h_i.

6. Use Exercise 5 to find

(a) g.c.d.(121,66)	(d) g.c.d.(2187,999)
(b) g.c.d.(169,273)	(e) g.c.d.(64,81)
(c) g.c.d.(51,187)	(f) g.c.d.(p^2q,pqr), where p, q, and r are primes.

7. Using the notation of Exercise 4, prove that

$$\text{l.c.m.}(a,b) = t_1^{j_1}t_2^{j_2} \ldots t_v^{j_v},$$

where each j_i is the largest of the corresponding g_i and h_i.

8. Do Exercise 4 of Section 2-2, using Exercises 5 and 7 of this section.

9. Use Exercise 7 to find

(a) l.c.m.(125,150)	(d) l.c.m.(253,506)
(b) l.c.m.(132,154)	(e) l.c.m.(111,1221)
(c) l.c.m.(39,143)	(f) l.c.m.(p^2q,pqr), where p, q, and r are primes.

10. For each finite set of integers $\{a,b,c,\ldots,r\}$, we can define

$$\text{g.c.d.}(a,b,c,\ldots,r)$$

to be the largest integer that divides each of a, b, c, . . . , and r. We can also define

$$\text{l.c.m.}(a,b,c,\ldots,r)$$

as the smallest integer that is divisible by each of a, b, c, . . . , and r. Find formulae for g.c.d.$(a,b,c, \ldots,r)$ and l.c.m.$(a,b,c, \ldots,r)$ by generalizing the assertions in Exercises 4, 5, and 7.

11. Find g.c.d.(39,102,75) and l.c.m.(39,102,75).

12. Prove that, if $d_1 = \text{g.c.d.}(a,b)$, $d_2 = \text{g.c.d.}(b,c)$, $d_3 = \text{g.c.d.}(c,a)$, $D = \text{g.c.d.}(a,b,c)$, and $L = \text{l.c.m.}(a,b,c)$, then

$$L = \frac{abcD}{d_1d_2d_3}.$$

CHAPTER 3

COMBINATORIAL AND COMPUTATIONAL NUMBER THEORY

Much of number theory is concerned with the properties of primes. In Chapter 2 we saw that these numbers are the multiplicative building blocks of the integers. In Sections 3–2 and 3–3, we shall use combinatorial techniques to obtain two surprising results about primes. The combinatorial ideas underlying this approach will also be used in proving many of the theorems in later chapters. In the fourth section, we shall introduce one of number theory's most useful tools, the generating function. To conclude the chapter, we shall discuss the role of computers in number theory.

3–1 PERMUTATIONS AND COMBINATIONS

Although permutations and combinations are usually associated with probability theory, they are also relevant to number theory. For instance, let us consider a problem that faces a number theorist each time he visits a Chinese restaurant.

Example 3–1: The Dinners for Two on a particular Chinese menu are presented as follows:

DINNERS FOR TWO

You may select one dish from each category.

Category A	Category B
Fung Wong Guy	Chicken Chow Mein
Wor Hip Har	Ho Yu Gai Poo
Moo Goo Guy Pen	

How many different Dinners for Two are available? Without any difficulty, we can list all the available dinners:

Fung Wong Guy and Chicken Chow Mein,
Fung Wong Guy and Ho Yu Gai Poo,
Wor Hip Har and Chicken Chow Mein,
Wor Hip Har and Ho Yu Gai Poo,
Moo Goo Guy Pen and Chicken Chow Mein, and
Moo Goo Guy Pen and Ho Yu Gai Poo.

Of course, we may easily count the dinners without listing them. We have 3 choices in Category A, and, after we make a decision there, we have 2 choices in Category B. Thus, without looking at the list, we note that there are

$$2+2+2=3\cdot 2=6$$

different dinners.

The simple counting procedure employed in Example 3–1 is a particular instance of the following fundamental rule.

GENERAL COMBINATORIAL PRINCIPLE: *If an element α can be chosen from a prescribed set S in m different ways, and if thereafter, a second element β can be chosen from a prescribed set T in n different ways, then the ordered pair (α,β) can be chosen in mn different ways.**

You may be wondering what all this can *really* have to do with number theory. The following examples lead us to expect that the product of any n consecutive positive integers is divisible by the product of the first n positive integers; though this assertion appears to have no direct relationship to combinatorial ideas, we shall see that the proof of it involves all the combinatorial concepts to be introduced in this section.

Example 3–2: For $n=4$, the product of the first four integers is $1\cdot 2\cdot 3\cdot 4=24$, and we observe that $5\cdot 6\cdot 7\cdot 8=1680=70\cdot 24$; also $10\cdot 11\cdot 12\cdot 13=17160=715\cdot 24$.

Example 3–3: For $n=5$, the product of the first 5 integers is $1\cdot 2\cdot 3\cdot 4\cdot 5=120$, and we observe that $4\cdot 5\cdot 6\cdot 7\cdot 8=6720=56\cdot 120$; also $11\cdot 12\cdot 13\cdot 14\cdot 15=360360=3003\cdot 120$.

*This principle is actually a theorem in the foundations of mathematics. See Theorem 10.4.12 in *The Anatomy of Mathematics* by Kershner and Wilcox.