It will be helpful to list some of the more 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:*

(1) $a \mid 0$, $1 \mid a$, $a \mid a$.
(2) $a \mid 1$ *if and only if* $a = \pm 1$.
(3) *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
(4) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
(5) $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.
(6) *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.
(7) *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

Proof: We shall prove assertions (6) and (7), 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 $|b| = |ac| = |a||c|$. Since $c \neq 0$, it follows that $|c| \geq 1$, whence $|b| = |a||c| \geq |a|$.

As regards (7), the relations $a \mid b$ and $a \mid c$ ensure that $b = ar$ and $c = as$ for suitable integers r and s. But then

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

whatever the choice of x and y. Since $rx + sy$ is an integer, this says that $a \mid (bx + cy)$, as desired.

It is worth pointing out that property (7) of the preceding theorem extends by induction to sums of more than two terms. That is, if $a \mid b_k$ for $k = 1, 2, \ldots, n$, then

$$a \mid (b_1 x_1 + b_2 x_2 + \cdots + b_n x_n)$$

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 $d \mid b$. Since 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 0, 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. Framed as a definition,

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

(1) $d \mid a$ and $d \mid b$,
(2) if $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 2-1

The positive divisors of -12 are 1, 2, 3, 4, 6, 12, while 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. Since 6 is the largest of these integers, it follows that $\gcd(-12, 30) = 6$. In the same way, one can show that

$$\gcd(-5, 5) = 5, \quad \gcd(8, 17) = 1, \quad \text{and} \quad \gcd(-8, -36) = 4.$$

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 $|a| = au + b \cdot 0$ will lie 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, one can obtain integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form

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

Were $r > 0$, 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 both a and b.

Now if c is an arbitrary positive common divisor of the integers a and b, then part (7) of Theorem 2-2 allows us to conclude that $c \mid (ax + by)$; in other words, $c \mid d$. By (6) 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 $ax + by$. Besides this, another fact can be deduced:

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: Since $d \mid a$ 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. On the other hand, 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 $d = \gcd(a, b)$. Since $d \mid a$ 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 $d = 1$ (part (2) 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 while a/d and b/d have the appearance of fractions, they are in fact integers since 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, one obtains the expression

$$1 = (a/d)x + (b/d)y.$$

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