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 $6 \cdot 8 \nmid 24$. Were 6 and 8 relatively prime, of course, this situation would not arise. This brings us to

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 it 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

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

Since $a \mid ac$ 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. 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*

(1) *$d \mid a$ and $d \mid b$,*
(2) *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 (1) 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 (2) 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 (2). The implication is that $d \geq c$, and consequently d is the greatest common divisor of a and b.

PROBLEMS 2.2

1. If $a \mid b$, show that $(-a) \mid b$, $a \mid (-b)$, and $(-a) \mid (-b)$.
2. Given integers a, b, c, verify that
   (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 $c \neq 0$.
3. Prove or disprove: if $a \mid (b + c)$, then either $a \mid b$ or $a \mid c$.
4. Prove that, for any integer a, one of the integers a, $a + 2$, $a + 4$ is divisible by 3. [*Hint:* By the Division Algorithm the integer a must be of the form $3k$, $3k + 1$, or $3k + 2$.]
5. (a) For an arbitrary integer a, establish that $2 \mid a(a + 1)$ while $3 \mid a(a + 1)(a + 2)$.
   (b) Prove that $4 \nmid (a^2 + 2)$ for any integer a.
6. For $n \geq 1$, use induction to show that
   (a) 7 divides $2^{3n} - 1$ and 8 divides $3^{2n} + 7$;
   (b) $2^n + (-1)^{n+1}$ is divisible by 3.
7. Show that if a is an integer such that $2 \nmid a$ and $3 \nmid a$, then $24 \mid (a^2 - 1)$.

8. Prove that
   (a) the sum of the squares of two odd integers cannot be a perfect square;
   (b) the product of four consecutive integers is one 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 that
    (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. 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.]
15. Establish each of the assertions below:
    (a) If a is an odd integer, then $24 \mid a(a^2 - 1)$. [*Hint:* The square of an odd integer is of the form $8k + 1$.]
    (b) If a and b are odd integers, then $8 \mid (a^2 - b^2)$.
    (c) If a is an integer not divisible by 2 or 3, then $24 \mid (a^2 + 23)$. [*Hint:* Any integer a must assume one of the forms $6k, 6k+1, \ldots, 6k+5$.]
    (d) If a is an arbitrary integer, then $360 \mid a^2(a^2 - 1)(a^2 - 4)$.
16. Confirm that the following properties of the greatest common divisor hold:
    (a) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
    [*Hint:* Since $1 = ax + by = au + cv$ 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 $d \mid b$.]

2.3 THE EUCLIDEAN ALGORITHM

The greatest common divisor of two integers can, of course, be found by listing all their positive divisors and picking out 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, it is today 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. Since $\gcd(|a|, |b|) = \gcd(a, b)$, 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 since 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 which appears in this manner, is equal to $\gcd(a, b)$. Our proof is based on the lemma below.

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