Proof: If $d = \gcd(a, b)$, then the relations $d \mid a$ and $d \mid b$ 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.

Although Theorem 2-3 asserts that $\gcd(a, b)$ can be expressed in the form $ax + by$, 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 backwards 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 2-2

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 above, namely the integer 6, is the greatest common divisor of 12378 and 3054:

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

In order 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 $y = -535$. It might be well to record that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054; among other possibilities, one 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 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 2-2, the smaller integer (namely 3054) has four digits, so that the total number of divisions cannot be greater than twenty; 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 in order to compute $\gcd(a_n, b_n)$ by the Euclidean Algorithm. We shall prove this fact in Chapter 13.

One more remark is necessary: The number of steps in the Euclidean Algorithm can usually 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 2-2, it would be 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 the above 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 31) is multiplied by k, we obtain

$$\begin{aligned} ak &= q_1(bk) + r_1 k, & 0 &< r_1 k < bk \\ bk &= q_2(r_1 k) + r_2 k, & 0 &< r_2 k < r_1 k \\ &\vdots \\ r_{n-2} k &= q_n(r_{n-1} k) + r_n k, & 0 &< r_n k < r_{n-1} k \\ r_{n-1} k &= q_{n+1}(r_n k) + 0. \end{aligned}$$

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 $r_n k$; that is,

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

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,

$$\gcd(ak, bk) = \gcd(-ak, -bk) = \gcd(a | k |, b \nmid k |) = | k | \gcd(a, b).$$

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 its 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, 0 is a common multiple of a and b. To see that common multiples which are not trivial do exist, 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

(1) $a \mid m$ and $b \mid m$,
(2) 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, $\operatorname{lcm}(-12, 30) = 60$.

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

What we lack is a relationship between the ideas of greatest common divisor and least common multiple. This gap is filled by

Theorem 2-8. *For positive integers a and b,*

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

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.