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,

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

This equation states that $m \mid c$, allowing us to conclude that $m \leq c$. Thus, in accordance with Definition 2-4, $m = \operatorname{lcm}(a, b)$; that is,

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

which is what we started out to prove.

Theorem 2-8 has a corollary that is worth a separate statement.

Corollary. *Given positive integers a and b,* $\operatorname{lcm}(a, b) = ab$ *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 its turn can be calculated from the Euclidean Algorithm. When considering the integers 3054 and 12378, for instance, we found that $\gcd(3054, 12378) = 6$; whence,

$$\operatorname{lcm}(3054, 12378) = \frac{3054 \cdot 12378}{6} = 6{,}300{,}402.$$

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 properties

(1) d is a divisor of each of a, b, c,
(2) if e divides the integers a, b, c, then $e \leq d$.

To cite two examples, we have

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

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 2.3

1. Find gcd (143, 227), gcd (306, 657) and gcd (272, 1479).

2. Use the Euclidean Algorithm to obtain integers x and y satisfying

   (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 $d \mid 2a$, $d \mid 2b$; 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 positive integers a, b and $n \geq 1$, show that

   (a) If $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$. [*Hint:* See Problem 16(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. For nonzero integers a and b, verify that the following conditions are equivalent:

   (a) $a \mid b$ (b) $\gcd(a, b) = |a|$ (c) $\operatorname{lcm}(a, b) = |b|$

7. Find lcm (143, 227), lcm (306, 657) and lcm (272, 1479).

8. Prove that the greatest common divisor of two positive integers always divides their least common multiple.

9. 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 $a = b$.
   (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.]

10. Let a, b, c be integers, no two of which are zero, and $d = \gcd(a, b, c)$. Show that

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

11. Find integers x, y, z satisfying

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

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

2.4 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. While Diophantus' works were written in Greek and he displayed the Greek genius for theoretical abstraction, he was most likely a Hellenized Babylonian. What personal particulars we have of his career come from the wording of an epigram-problem (apparently dating from the 4th century) to the effect: 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 four years after his son. If x was the age at which Diophantus died, these data lead to the equation

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

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 out 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 our sense. 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.

It is customary to apply the term *Diophantine equation* to any equation in one or more unknowns which 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 not both zero. A solution of this equation is a pair of integers x_0, y_0 which, 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 dealt with finding squares or cubes with certain properties.

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

$$3 \cdot 4 + 6 \cdot 1 = 18,$$
$$3(-6) + 6 \cdot 6 = 18,$$
$$3 \cdot 10 + 6(-2) = 18.$$

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, while the right-hand side is not. Faced with this, it is reasonable to inquire 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 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.