Because $(a, -b) = (-a, b) = (-a, -b) = (a, b)$, we confine our discussion of gcds to positive integers.

How do we know the gcd of a and b always exists? Since $1|a$ and $1|b$, 1 is a common divisor of a and b, so they have at least one common divisor. If d' is a common divisor, then $d' \leq a$ and $d' \leq b$, so $d' \leq \min\{a, b\}$; that is, every common divisor is bounded by a positive integer, namely, the smaller of a and b. Therefore, by the well-ordering principle, the set of common factors contains a largest element d, so (a, b) exists.

Next question, is the gcd of a and b unique? It is, so we can talk about *the* gcd of a and b (see Exercise 50).

The preceding verbal definition of gcd, although simple and clear, is not a practical one, so we rewrite it symbolically.

A Symbolic Definition of gcd

A positive integer d is the gcd of two positive integers a and b if

- $d|a$ and $d|b$, and
- if $d'|a$ and $d'|b$, then $d' \leq d$, where d' is also a positive integer.

Thus $d = (a, b)$ if two conditions are satisfied:

- d must be a common factor of a and b.
- d must be the largest common factor of a and b; in other words, any other common factor d' must be $\leq d$.

An Explicit Formula for gcd

In 1997, Marcelo Polezzi of Brazil employed a geometric approach to derive an explicit formula for computing the gcd d of a and b, given by the following theorem. Its proof involves counting the **lattice points** (x, y) on the Cartesian plane, which are points with integral coordinates x and y.

THEOREM 3.1 (M. Polezzi, 1997) Let $d = (a, b)$. Then

$$d = 2\sum_{i=1}^{a-1} \left\lfloor i\frac{b}{a} \right\rfloor + a + b - ab.$$

PROOF

We count the lattice points on and inside $\triangle AOB$ in Figure 3.1 in two ways, where line $\overleftrightarrow{AB}$ is given by $y = -(b/a)x + b$.

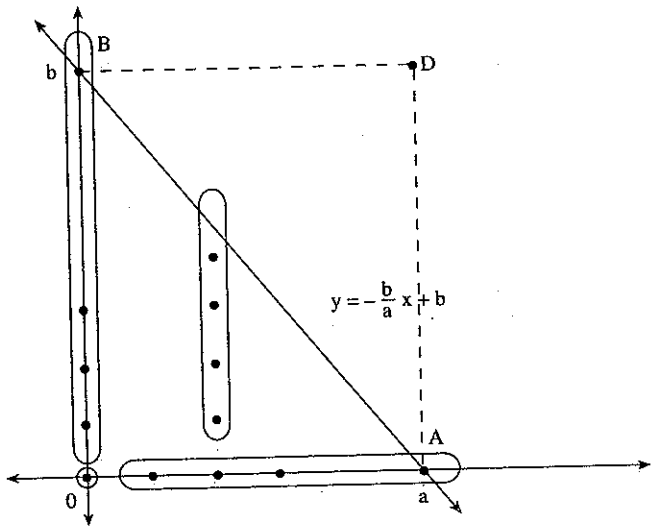

Figure 3.1

Number of lattice points on the legs of $\triangle AOB = a + b + 1$

$$\text{Number of lattice points inside or on the hypotenuse} = \sum_{i=1}^{a-1} \left\lfloor -i\frac{b}{a} + b \right\rfloor$$

$$= \sum_{i=1}^{a-1} \left\lfloor (a-i)\frac{b}{a} \right\rfloor$$

$$= \sum_{i=1}^{a-1} \left\lfloor i\frac{b}{a} \right\rfloor$$

$$\therefore \quad \text{No. of lattice points } s \text{ on or inside } \triangle AOB = \sum_{i=1}^{a-1} \left\lfloor i\frac{b}{a} \right\rfloor + (a+b+1)$$

(See Figure 3.2 for $a = 6$ and $b = 9$.)

No. of lattice points on $\overline{AB}$

= no. of points (x, y), where x and $y = -\frac{b}{a}x + b$ are integers.

= no. of integers x such that $y = -\frac{b}{a}x + b$ is an integer, where $0 \le x \le a$

$$= \text{no. of integers in the set } \left\{0, \frac{a}{d}, \frac{2a}{d}, \ldots, \frac{(d-1)a}{d}, a\right\}$$

$= d + 1$

(See Figure 3.3 for $a = 6$ and $b = 9$.)

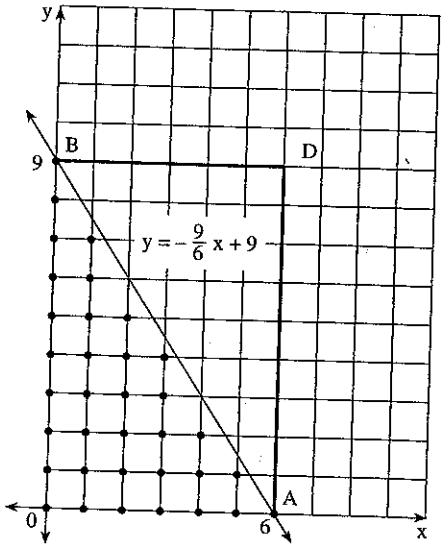

Figure 3.2 *Lattice points on or inside* $\triangle AOB$ *for* $a = 6$ *and* $b = 9$.

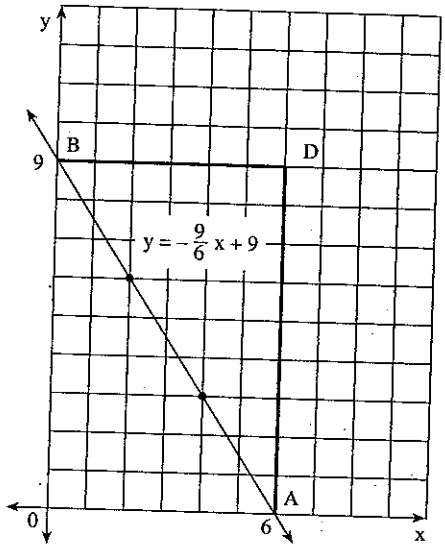

Figure 3.3 *Lattice points on AB for* $a = 6$ *and* $b = 9$.

$\therefore$ No. of lattice points inside $\triangle ADB$ or on its legs equals $s - (d + 1)$.
Total no. of points on or inside the rectangle $OADB = s + [s - (d + 1)]$
$= 2s - (d + 1)$
But the total no. of lattice points on or inside the rectangle $= (a + 1)(b + 1)$
Thus $2s - (d + 1) = (a + 1)(b + 1)$. Solving this equation, we get

$$d = 2s - (a + 1)(b + 1) - 1$$
$$= 2\sum_{i=1}^{a-1} \left\lfloor i\frac{b}{a} \right\rfloor + a + b - ab$$

This formula works even if $b = 0$. ■

The following example demonstrates this formula.

EXAMPLE 3.1 Use Theorem 3.1 to compute (18, 24).

SOLUTION

$$(18, 24) = 2\sum_{1}^{17} \left\lfloor i\frac{24}{18} \right\rfloor + 18 + 24 - 18 \cdot 24 = 2\sum_{1}^{17} \left\lfloor i\frac{4}{3} \right\rfloor - 390$$
$$= 2(1 + 2 + 4 + 5 + 6 + 8 + 9 + 10 + 12 + 13 + 14 + 16 + 17 + 18$$
$$+ 20 + 21 + 22) - 390 = 6$$

■