### 11.1.6 Solving Equations

**Diophantine Equations** A *Diophantine equation* is an equation of the form

$$ax + by = c,$$

where $a$, $b$, and $c$ are constants and the values of $x$ and $y$ should be found. Each number in the equation has to be an integer. For example, one solution to the equation

$$5x + 2y = 11$$

is $x = 3$ and $y = -2$.

We can efficiently solve a Diophantine equation by using the extended Euclid's algorithm (Sect. 11.1.3) which gives integers $x$ and $y$ that satisfy the equation

$$ax + by = \gcd(a, b).$$

A Diophantine equation can be solved exactly when $c$ is divisible by $\gcd(a, b)$.

As an example, let us find integers $x$ and $y$ that satisfy the equation

$$39x + 15y = 12.$$

The equation can be solved, because $\gcd(39, 15) = 3$ and $3 \mid 12$. The extended Euclid's algorithm gives us

$$39 \cdot 2 + 15 \cdot (-5) = 3,$$

and by multiplying this by 4, the equation becomes

$$39 \cdot 8 + 15 \cdot (-20) = 12,$$

so a solution to the equation is $x = 8$ and $y = -20$.

A solution to a Diophantine equation is not unique, because we can form an infinite number of solutions if we know one solution. If a pair $(x, y)$ is a solution, then also all pairs

$$\left(x + \frac{kb}{\gcd(a, b)}, y - \frac{ka}{\gcd(a, b)}\right)$$

are solutions, where $k$ is any integer.

**Chinese Remainder Theorem** The *Chinese remainder theorem* solves a group of equations of the form

$$\begin{aligned} x &= a_1 \bmod m_1 \\ x &= a_2 \bmod m_2 \\ &\cdots \\ x &= a_n \bmod m_n \end{aligned}$$