Solving Linear Congruence

A equation of the form

$$ax \equiv b \pmod{m}$$

where a, b, m are positive integers and x is a variable is called a **linear congruence**. If we assume that

$$\gcd(a, m) = 1$$

then the equation has infinitely many solutions. We can find all solutions as follows.

1. Using Euclid's extended algorithm, we find an integer x_0 such that
$$ax_0 \equiv 1 \pmod{m}. \tag{1}$$
Such an x_0 is called an **inverse** of a modulo m.

2. Multiplying equation (1) by b, we obtain
$$a(x_0 b) \equiv b \pmod{m}$$
so that $x = x_0 b$ is a solution of the linear congruence.

3. For any integer k, $\boxed{x = x_0 b + mk}$ is a solution of the linear congruence. The number
$$x = x_0 b \bmod m$$
is the unique solution over $0 \leq x < m$.

To illustrate this, let's find all solutions of

$$9x \equiv 15 \pmod{23} \tag{2}$$

and identify the unique solution over $0 \leq x < 23$.

Let's first use Euclid's algorithm to find $\gcd(23, 9)$.

$$\begin{aligned} 23 &= 9(2) + 5 \\ 9 &= 5(1) + 4 \\ 5 &= 4(1) + \boxed{1} \longleftarrow \gcd(23, 9) \\ 4 &= 1(4) + 0 \end{aligned}$$

Using back substitution we obtain

$$\begin{aligned} 1 &= 5 - \mathbf{4} \\ &= 5 - \boxed{(9 - 5)} = \mathbf{5}(2) - 9 \\ &= \boxed{(23 - 9(2))}(2) - 9 = 23(2) - 9(5) \end{aligned}$$

The last equation implies that

$$9(-5) = 1 + 23(-2) \longrightarrow 9(-5) \equiv 1 \pmod{23}. \tag{3}$$

We conclude that $x_0 = -5$ is an inverse of 9 modulo 23.

Multiplying equation (3) by 15 we obtain

$$9(-75) \equiv 15 \pmod{23}.$$

Then, for any integer k, $\boxed{x = -75 + 23k}$ are solutions of the linear congruence (2). The unique solution in $0 \leq x < 23$ is

$$x = -75 \bmod 23 = 17.$$