Linear Congruence Equation

Table of Contents

This equation is of the form:

$$a \cdot x = b \pmod{n},$$

where a, b and n are given integers and x is an unknown integer.

It is required to find the value x from the interval $[0, n-1]$ (clearly, on the entire number line there can be infinitely many solutions that will differ from each other in $n \cdot k$, where k is any integer). If the solution is not unique, then we will consider how to get all the solutions.

Solution by finding the inverse element

Let us first consider a simpler case where a and n are **coprime** ($\gcd(a, n) = 1$). Then one can find the

inverse of a, and multiplying both sides of the equation with the inverse, and we can get a **unique** solution.

$$x = b \cdot a^{-1} \pmod{n}$$

Now consider the case where a and n are **not coprime** ($\gcd(a, n) \neq 1$). Then the solution will not always exist (for example $2 \cdot x = 1 \pmod{4}$ has no solution).

Let $g = \gcd(a, n)$, i.e. the greatest common divisor of a and n (which in this case is greater than one).

Then, if b is not divisible by g, there is no solution. In fact, for any x the left side of the equation $a \cdot x \pmod{n}$, is always divisible by g, while the right-hand side is not divisible by it, hence it follows that there are no solutions.

If g divides b, then by dividing both sides of the equation by g (i.e. dividing a, b and n by g), we receive a new equation:

$$a' \cdot x = b' \pmod{n'}$$

in which a' and n' are already relatively prime, and we have already learned how to handle such an equation. We get x' as solution for x.

It is clear that this x' will also be a solution of the original equation. However it will **not be the only solution**. It can be shown that the original equation has exactly g solutions, and they will look like this:

$$x_i = (x' + i \cdot n') \pmod{n} \quad \text{for } i = 0 \dots g-1$$

Summarizing, we can say that the **number of solutions** of the linear congruence equation is equal to either $g = \gcd(a, n)$ or to zero.

Solution with the Advanced Euclidean Algorithm

We can rewrite the linear congruence to the following Diophantine equation:

$$a \cdot x + n \cdot k = b,$$

where x and k are unknown integers.

The method of solving this equation is described in the corresponding article Linear Diophantine equations and it consists of applying the Extended Euclidean Algorithm.

It also describes the method of obtaining all solutions of this equation from one found solution, and incidentally this method, when carefully considered, is absolutely equivalent to the method described in the previous section.