Modular linear equation of the first order

Statement of the Problem

This equation of the form:

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

where a, b, n- given integers, x- unknown integer.

Required to find the desired value $x$lying in the interval $[0; n-1]$(as on the real line, it is clear there can be infinitely many solutions, which will be different for each other $n \cdot k$, where k- any integer). If the solution is not unique, then we'll look at how to get all solutions.

The decision by finding the inverse element

Consider first the simplest case - when $a$and **coprime** . Then we can find the inverse of a number , and multiplying on both sides of it, to obtain a solution (and it will be **the only**):n a

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

Now consider the case $a$and **are not relatively prime** . Then, obviously, the decision will not always exist (for example).n $2 \cdot x = 1 \pmod{4}$

Suppose $g = \gcd(\mathrm{a}, \mathrm{n})$, that their greatest common divisor (which in this case is greater than one).

Then, if $b$not a multiple of g, the solutions do not exist. In fact, for any $x$left-hand side of the equation, ie $(a \cdot x) \pmod{n}$, always divisible by g, while the right side of it is not divisible, which implies that there are no solutions.

If it $b$is divisible by g, then dividing both sides by it g(ie, dividing a, $b$and $n$on g), we arrive at a new equation:

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

where $a'$and $n'$are relatively prime already, and this equation we have learned to solve. We denote its solution through x'.

It is understood that this x'will also be a solution of the original equation. However, if $g > 1$, it is **not the only** solution. It can be shown that the original equation will have exactly $g$the decisions and they will look like:

$$x_i = (x' + i \cdot n') \pmod n,$$

$$i = 0 \ldots (g-1).$$

Summarizing, we can say that **the number of solutions** of a linear equation is either modular $g = \gcd(\mathrm{a}, \mathrm{n})$or zero.

Solution using the Extended Euclidean algorithm

We present our modular equation to Diophantine equation as follows:

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

where $x$and k- unknown integers.

The method of solving this equation is described in the relevant article of linear Diophantine equations of the second order , and it is in the application of the Extended Euclidean algorithm .

There also described a method for obtaining all solutions of this equation one solution found, and, by the way, this way on closer examination is equivalent to the method described in the preceding paragraph.