added: 11 Jul 2008 10:35
Edited: 8 Sep 2010 21:21

Modular linear equation of the first order

Contents [hide]

Statement of the Problem

This equation of the form:

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

where a, b, n- given integers, x- the 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 that are different to each other on $n \cdot k$where k- any integer). If the solution is not unique, then we will see how to get all the solutions.

Solution by finding the inverse element

Consider first the simplest case - when $a$and **are relatively prime** . Then we can find the inverse of a number , and multiplying it by both sides of the equation to get 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 $g = \gcd(a, n)$, that is, their greatest common divisor (which in this case is greater than one).

Then, if $b$not divisible by $g$then no solution exists. In fact, if any $x$left side of the equation, i.e. $(a \cdot x) \pmod n$, is always divisible by g, while the right part it is not divided, 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'already be relatively prime, and this equation we have learned to solve. We denote its solution through x'.

Clearly, this x'will also be a solution of the original equation. If, however $g > 1$, 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:

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

To summarize, we can say that **the number of solutions** of linear modular equations is either $g = \gcd(a, n)$, or zero.

Solution with the Extended Euclidean algorithm

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