Algologic Technical Report # 01/2017

Modulo of a negative number[1]

S. Parthasarathy
drpartha@gmail.com

Ref.: negamodulo.tex
Ver. code: 20170109e

Abstract

This short article discusses an enigmatic question in elementary number theory – that of finding the modulo of a negative number. Is this feasible to compute ? If so, how do we compute this value ?

1 Modular arithmetic

In mathematics, modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value - the modulus (plural moduli). The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book Disquisitiones Arithmeticae, published in 1801. Modular arithmetic is a fascinating aspect of mathematics. The "modulo" operation is often called as the fifth arithmetic operation, and comes after $+ - * \; and \; /$. It has use in many practical situations, particularly in number theory and cryptology [1] [2].

If x and n are integers, $n < x$ and $n \neq 0$, the operation " x mod n " is the remainder we get when n divides x. In other words,

$(x \bmod n) = r$ if there exists some integer q such that

$x = q * n + r$

[1]This is a LaTeX document. You can get the LaTeX source of this document from drpartha@gmail.com. Please mention the Reference Code, and Version code, given at the top of this document

When r = 0 , n is a factor of x. When n is a factor of x, we say n divides x evenly, and denote it by $n \mid x$.

The modulo operation can be combined with other arithmetic operators. We can compute $(A + B) \bmod n$

The associativity rule of normal arithmetic is modified slightly, to give:

$$(A + B) \bmod n \ = (\ A \bmod n \ + \ B \bmod n) \bmod n \tag{1}$$

An interesting observation we can make, based on the above, is that

$$A \ mod \ n \ + \ ((-A) \ mod \ n) \ = \ n \tag{2}$$

Thus,

$$(A \ mod \ n \ + \ ((-A) \ mod \ n)) \mod n = n \mod n \quad = 0 \tag{3}$$

Let us try a simple example. We know that $52 \ mod \ 13 \ = \ 0$, since 13 divides 52 evenly (without a remainder). Now, let us evaluate $(47 \ + \ 5) \ mod \ 13$ using the identity given above.

$$\begin{aligned} 52 \ mod \ 13 &= \ (47 \ + \ 5) \ mod \ 13 && (4)\\ &= \ (47 \ mod \ 13 \ + \ 5 \ mod \ 13) \ mod \ 13 && (5)\\ &= (8 + 5) \ mod \ 13 && (6)\\ &= \ 0 && (7) \end{aligned}$$

In the above example, 5 *mod* 13 behaves like the *modular additive inverse mod 13* of 47 *mod* 13

However, this can lead to a riddle-like situation, as explained below.

2 The modulo riddle

In normal arithmetic, $A - B$ can be written as:

$A \ + \ (-B)$
or as
$A \ - \ (+B)$

Consider the following expression in modulo arithmetic :

$$(A - B)\ mod\ n \tag{8}$$

Are the following expressions equivalent to the above expression?

$$((A\ mod\ n) + (-B\ mod\ n))\ mod\ n \tag{9}$$

$$((A\ mod\ n) - (B\ mod\ n))\ mod\ n \tag{10}$$

3 The solution

The answer is YES.

To justify the above answer , we must see how is (-B mod n) calculated, i.e., how is the mod of a negative number calculated ?

It is calculated exactly like the mod of a positive number.

$(x \text{ mod } n) = r$ if there exists some integer q such that

$$x = q * n + r$$

Rearranging the terms, we get :

$$x - q * n = r$$

Notice that since x is a negative integer in the present case, q is currently a negative integer. Therefore to find $-x\ mod\ n$, just keep adding n to x until the result is between 0 and n

As an example, let us evaluate $x\ mod\ n$ where $n = 13, x = -27$. Add 13 to -27, you get -14, add again, you get -1, and add again, you get 12. Thus,

$$-27\ mod\ 13 = 12$$

Let us now compute $(47 - 27)\ mod\ 13$. This is obviously:

$$20\ mod\ 13\ =\ 7 \tag{11}$$

Now, let us compute $(47 - 27)\ mod\ 13$ using the two expressions 9 and 10 given above.

3.1 Using $((A \ mod \ n) + (-B \ mod \ n)) \ mod \ n$

Substituting A, B , and n appropriately in the above expression, we get:

$$\begin{aligned} ((47 \ mod \ 13) + (-27 \ mod \ 13)) \ mod \ 13 &= (8 \ + \ 12) \ mod \ 13 && (12) \\ &= \ (20) \ mod \ 13 && (13) \\ &= \ 7 && (14) \end{aligned}$$

3.2 Using $((A \ mod \ n) - (B \ mod \ n)) \ mod \ n$

Substituting A, B , and n appropriately in the above expression, we get:

$$\begin{aligned} ((47 \ mod \ 13) - (27 \ mod \ 13)) \ mod \ 13 &= (8 \ - \ 1) \ mod \ 13 && (15) \\ &= \ (7) \ mod \ 13 && (16) \\ &= \ 7 && (17) \end{aligned}$$

It all falls in place at last ! Amen.

4 Wrapup

The above article uses specific examples to highlight some aspects of modular arithmetic. These are not "proofs" in a strict mathematical sense. The formal proofs are left as an exercise for the diligent reader.

If you find this article useful, please send a note to drpartha@gmail.com. Comments, suggestions and remarks are always welcome, as long as they are constructive.

This article, as well as other similar articles can be downloaded from [3]

References

[1] K. H. Rosen, Discrete Mathematics and its applications, Tata McGraw-Hill Publishing Company, India.

[2] V. K. Krishnan, Elementary number theory, Pub.: Universities Press, India.

[3] S. Parthasarathy, http://drpartha.org.in/publications/downloadables.htm

***