MODULAR ARITHMETIC

Modular arithmetic is basically doing addition (and other operations) not on a line, as you usually do, but on a circle -- the values "wrap around", always staying less than a fixed number called the modulus.

Modular arithmetic is a system of **arithmetic** for integers, where values reset to zero and begin to increase again, after reaching a certain predefined value, called the modulus (**modulo**). **Modular arithmetic** is widely used in computer science and **cryptography**.

For example: Mod-arithmetic is the central mathematical concept in cryptography. Almost any cipher from the Caesar Cipher to the RSA Cipher use it.

Modular or clock arithmetic is arithmetic on a circle instead of a number line modulo N , we use only the twelve whole numbers from 0 through N-1.

Example 2:

When 8 is divided by 3 it leaves a remainder of 2. Thus, we write:

$$8 \bmod 3 = 2.$$

$$-11 \bmod 7 = 3.$$

Introduction to Modular Math

When we divide two integers we will have an equation that looks like the following:
wing:

A/*B*=*Q* remainder *R*

A is the dividend
B is the divisor
Q is the quotient
R is the remainder

For these cases there is an operator called the **modulo operator (abbreviated as mod).**
Using the same A, B, Q, and R as above, we would have: A mod B = R

We would say this as A *modulo* B *is equal to* R. Where B is referred to as the modulus.

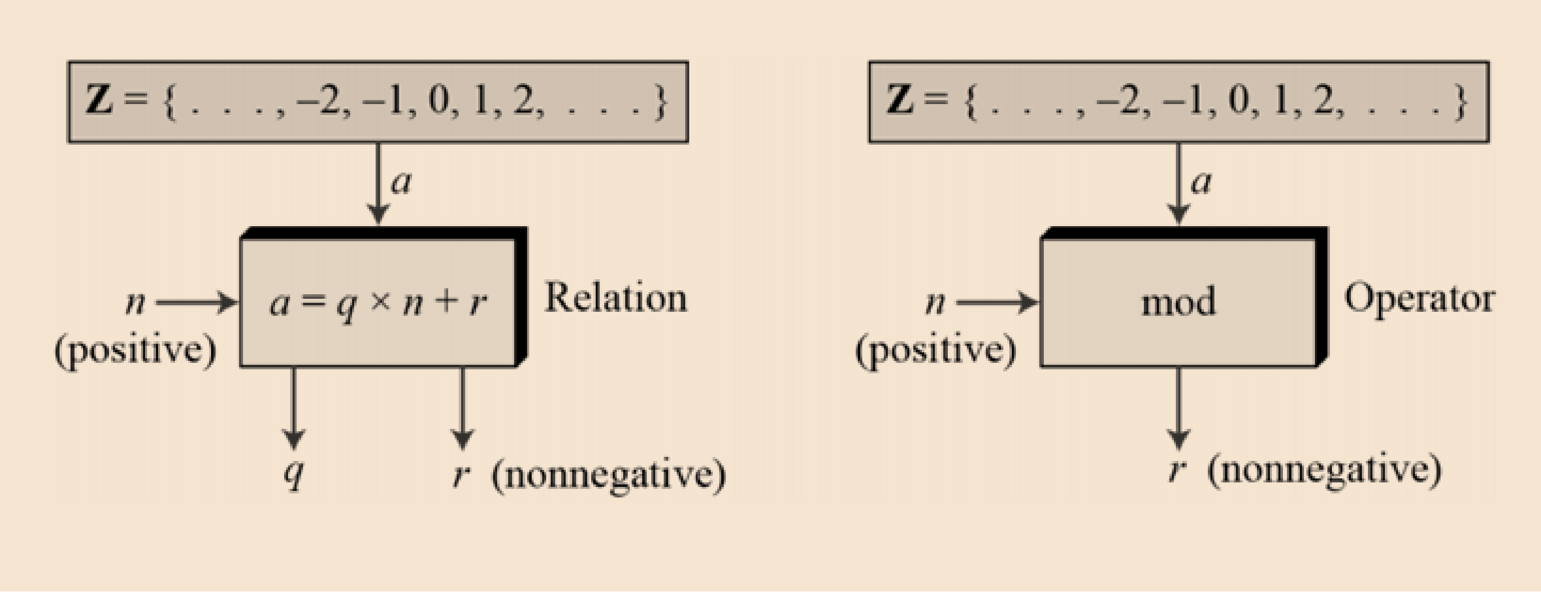
For example:
13/5=2 remainder 3
13 MOD 5=3

The division relationship (a = q × n + r) discussed in the previous section has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r.

Modulo Operator

The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.

The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.



How to find a modulus of negative number

Method1:
N(mod m)

N=q*m+R **(we have to choose “q” such that we get a more –ve number than “n” or the same –ve number).**

Example: -11 mod 7 **find: -15 mod 7=???**
N(mod m)
N=-11
M=7
N=q*m+R
-11=q*7+R
q??
q=-2
-11=-2*7+R
R(reminder)=10

Method 2:

-x mod y= y-(x mod y)

Example 1:

-51 mod 10

-x=51

Y=10

10-(51%10)

10-1

9

Note: -x mod y = y-(x mod y)

If |x| mod y!=0 it works

i.e |x| mod y==0 it fails -number

Example2:

-11 mod 7=3.

Solution:

7-(11%7)=7-4=3

Task:

0 mod 7

1 mod 7

2 mod 7

3 mod 7

4 mod 7

6 mod 7

7 mod 7

8 mod 7

9 mod 7

10 mod 7

-17 mod 10?

-61 mod 5

-35 mod 5?