Integer Arithmetic

Gunjan.Rehani@bennett.edu.in, Madhushi.Verma@bennett.edu.in

CSE, SEAS
Bennett University

June 15, 2021

Overview

Relatively Prime Integers

Two integers a and b are said to be relative prime or co-prime if gcd(a,b)=1

e.g Two numbers 16 and 21 are relatively prime as gcd(16,21)=1

1. 15,28 are relatively prime?
2. 32,63 are relatively prime?

Note: If a and b are relative primes then there exists integer x and y such that ax+by=1(gcd of a and b).

As an example, the greatest common divisor of 5 and 3 is 1, and we can write 5*(2)+3*(-3)=1.

a mod n=r
here a is any integer Z, n should be a positive integer and r should be non-negative.
n is called "modulus" and r is called the "residue".
Examples
A) 27 mod 5 =2
B) 36 mod 12=0
C) -18 mod 14=-4
Here r is negative. So to make it non-negative, add the modulus.
-4+14=10
therefore r=10
D) -7 mod 10=-7=-7+10=3

Set of Residues : Z_n

The result of the modulo operation with modulus n is always an integer between 0 and n-1.
That is, the result is always a non-negative integer less than n.
Therefore, the modulus operation creates a set called the set of least residues modulo n or Z_n.
$Z_n = \{0, 1, 2, 3, ..., (n-1)\}$
e.g. $Z_2 = \{0, 1\}$
$Z_6 = \{0, 1, 2, 3, 4, 5\}$
$Z_{11} = \{0, 1, 2, .., 10\}$

Congruence

Let a and b be integers. Then $a \equiv b \pmod{m}$ is read as " a is congruent to b modulo m"
This means that they both leave the same remainder when divided by m.
e.g. $2 \equiv 12 \pmod{10}$
$-8 \equiv 2 \pmod{5}$
$Z_{10}=\{0,1,2,3,4,5,6,7,8,9\}$
$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$

Properties of Congruence

Let a,b,c and d be integers.Then following are the properties of Congruence Relation.

1. If $a \equiv b \pmod{m}$, then $b \equiv a (\text{mod m})$
2. If $a \equiv b \pmod{m}$ and $b \equiv c (\text{mod m})$, then $a \equiv c \pmod{m}$
3. If $a \equiv b \pmod{m}$ and $c \equiv d (\text{mod m})$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$
4. If $a \equiv b \pmod{m}$, then $ac \equiv bc (\text{mod m})$
5. If $a \equiv b \pmod{m}$, then $a^k \equiv b^k (\text{mod m})$, for all $k \geq 1$

Residue Classes

Let m be a positive integer and a be any integer, then
$[a]_m = \{x : x \equiv a (mod m)\}$
e.g. if m=5, we have 5 sets
[0],[1],[2],[3],[4]
$[0] = \{..., -15, -10, 0, 5, 10, 15, ...\}$
$[1] = \{..., -14, -9, -4, 1, 6, 11, 16, ...\}$
$[2] = \{..., -13, -8, -3, 2, 7, 12, 17...\}$
$[3] = \{..., -12, -7, -2, 3, 8, 13, 18...\}$
$[4] = \{..., -11, -6, -1, 4, 9, 14, 19...\}$

Operations in Z_n

A) (a+b) mod n
B) (a-b) mod n
C) ($a \times b$) mod n
e.g.

1. Add 7 to 14 in Z_{15}
2. Subtract 11 from 7 in Z_{13}
3. Multiply 11 by 7 in Z_{20}

Properties

1. (a+b) mod n=[(a mod n) +(b mod n)]mod n
2. (a-b) mod n=[(a mod n) -(b mod n)]mod n
3. $(a \times b)$ mod n=[(a mod n)$\times$ (b mod n)]mod n