Lecture-2

Date

Page

Note: a and b are Multiplicative Inverse if (with respect to MOD n)

$$(a * b) \text{ MOD } n = 1$$

Identity of *

Note: a and b are additive Inverse with respect to MOD n if

$$(a + b) \text{ MOD } n = 0$$

Identity of +

E.g. $a = 23$, $b = 3$ } are additive Inverse of each other with respect to MOD 26.

because $(23 + 3) \text{ MOD } 26$

$= 26 \text{ MOD } 26$

$= 0$

For 4, 22 is additive Inverse

Note: It is always possible to find Additive Inverse with respect

Date______
Page______

Note: It is not always possible to find Multiplicative Inverse of 'a' with respect to MOD n

↓ why?

Because for Multiplicative Inverse to exist, necessary condition is $\gcd(a, n) = 1$.

★ How many numbers from the range of MOD 26 have Multiplicative Inverse?

1	✓	14	✗
2	✗	15	✓
3	✓	16	✗
4	✗	17	✓
5	✓	18	✗
6	✗	19	✓
7	✓	20	✗
8	✗	21	✓
9	✓	22	✗
10	✗	23	✓
11	✓	24	✗
12	✗	25	✓
13	✗	0	✗

Note: There are total 12 numbers from 0 to 25 whose Multiplicative Inverses are possible.

Note: Why $0^{-1} \bmod 26$ is not possible?

Because $\gcd(0, 26)$

$0 = 0 \times 26$

$26 = 1 \times 26$

$\therefore \boxed{\gcd(0, 26) = 26} \neq 1$

$\therefore 0^{-1} \bmod 26$ Doesn't exist.

Remember

$$\boxed{\begin{array}{l} \gcd(a, 0) = a \\ \gcd(a, 1) = 1 \end{array}}$$

Few Mathematical Notations:

(1) $Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$

→ Set of Integers from 0 to $(n-1)$
→ It is also the range of numbers obtained by performing MOD n over any number.

E.g. $Z_5 = \{0, 1, 2, 3, 4\}$

(2) $Z_n^* =$ Set of all numbers 'a' such that $\gcd(a, n) = 1$

$= \{ a / \gcd(a, n) = 1$ where 'a' is from 0 to $(n-1) \}$

Actually '0' is never possible

$\therefore Z_n^* = \{ a / \gcd(a, n) = 1$ where 'a' is from 1 to $(n-1) \}$

It can also be viewed as set of numbers from Z_n whose multiplicative Inverses are possible.

$\therefore Z_{26}^{*} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$|Z_{26}^{*}| = 12$

Cardinality of Z_{26}^{*} i.e. Number of Elements in Z_{26}^{*}

$|Z_{26}^{*}|$ is also known as $\phi(26)$

i.e. $|Z_{26}^{*}| = 12 = \phi(26)$

Euler's Totient Function

* following rule helps to find the value of $\phi(n)$

① $\phi(1) = 1$

② $\phi(p) = p-1$ if p is a prime

③ $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime

④ $\phi(p^e) = p^e - p^{e-1}$ if p is a prime

Ex: $|Z_{26}^*| = \phi(26)$

$= \phi(2 \times 13)$

$= \phi(2) \times \phi(13)$

$= (2-1) \times (13-1)$

$= 12$

Ex: $\phi(16) = \phi(2^4)$

$= 2^4 - 2^{4-1}$

$= 8$

$Z_{16} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$

$Z_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$

3) $(a \pm b) \bmod n$

$$= (a \bmod n \pm b \bmod n) \bmod n$$

) $(a * b) \bmod n$

$$= (a \bmod n * b \bmod n) \bmod n$$

$$a^m \bmod n$$

$$= [a \bmod n]^m \bmod n$$

$$LHS = a^m \bmod n$$

$$= (\underbrace{a * a * \ldots * a}_{m \text{ times}}) \bmod n$$

$$= [(a \bmod n) * (a \bmod n) * \ldots * (a \bmod n)] \bmod n$$

$$= (a \bmod n)^m \bmod n$$

$$= RHS$$

☆ 'a' and 'b' are congruent with respect to MOD n if

$$a \bmod n = b \bmod n$$

In general, written as

$$a \equiv b \pmod n$$

Congruence Relation symbol