Sbt lec after mids

18-5-2022

DMS

Congurence is a way of writing modulus

$19 \equiv 1 \text{ Mod } 3$

$4 \equiv 1 \text{ Mod } 3$

$11 \equiv 1 \text{ Mod } 2$

$Z = -\infty \quad 0 \quad +\infty$

$Z \text{ mod } 2$

$35 \equiv 1 \text{ Mod } 2$
$36 \equiv 0 \text{ Mod } 2$
$37 \equiv 1 \text{ Mod } 2$
$\vdots \quad \vdots \quad \vdots \quad \vdots$

In this way integers are divided into two parts

$Z_2 = \{0, 1\}$

$\downarrow$ $\hookrightarrow$ odd class of $Z = \infty$

even class of integer $= \infty$

$Z_3 = \{0, 1, 2\}$

35 Mod 3

$$\begin{array}{r|l} & 11 \\ 3 & 35 \\ & \underline{33} \\ & 2 \end{array}$$

$35 \equiv 2 \text{ Mod } 3$

$Z_n = Z \bmod n$

- If n numbers in Z
- Then ~~Lot~~ classes $n-1$ $+ 0$

$0 \rightarrow n-1$

Modular Arithemetic

Modular Addition

$3 \text{ Mod } 5 + 4 \text{ Mod } 5 = (3+4) \text{ Mod } 5$
$= 7 \text{ Mod } 5$
$= 2 \text{ Mod } 5$

- It will belong to class set of 5

Closure Property ***

If we perform modular addition then, our result belong to class set ~~of~~ then we say it is closed under addition

Modular Subtraction

$3 \text{ Mod } 7 - 6 \text{ Mod } 7$
$-3 \text{ Mod } 7 = 4 \text{ Mod } 7$

2 Mod 7 - 6 Mod 7

(2 - 6) Mod 7

-4 Mod 7 ⇒ 3 Mod 7

Modular Multiplication

4 Mod 7 x 5 Mod 7

(4x5) Mod 7

20 Mod 7

⇒ 6 Mod 7

5 Mod 7 * 6 Mod 7

30 Mod 7

⇒ 2 Mod 7

Each class of z is repesented by smallest non-negative integer.

→ Always rep mod in term of smallest non-negative integer.

Encryption

Tot eng alpha = 26

⇒ CAT

secret key = 9

$Z_{26} = [0 \rightarrow 25]$

Trick

A	F	K	P	U	Z
0	5	10	15	20	25

C	A	T
↓	↓	↓
2	0	19

$y = (x+k) \text{ Mod } 26$

$= (2+9) \text{ Mod } 26$

$= 11 \text{ Mod } 26$

$\cancel{= 4 \text{ Mod } 26}$

$y_1 = 11 \text{ Mod } 26$

$11 \Rightarrow L$

$y_2 = (0+9) \text{ Mod } 26$

$= 9 \text{ Mod } 26$

$9 \Rightarrow J$

$y_3 = 19+9 \text{ Mod } 26$

$= 28 \text{ Mod } 26$

$= 2 \text{ Mod } 26$

$2 \Rightarrow C$

Encrypted cat = LJC

Decryption

L J C

Key = 9

$x_1 = (11-9) \text{ Mod } 26$
$= 2 \text{ Mod } 26$

$2 = C$

$x_2 = (9-9) \text{ Mod } 26$
$= 0 \text{ Mod } 26$
$\hookrightarrow A$
$0 = A$

$x_3 = (2-9) \text{ Mod } 26$
$= -7 \text{ Mod } 26$
$= 19 \text{ Mod } 26$
$19 = T$

L J C = CAT

AES = Advanced encryp standards

Modular division

⇒ Additive Inverse

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

Additive inverse of 2 Mod 7

(2 + 5) Mod 7 = 7 Mod 7

= 0 Mod 7

↓

+ve

from class set of 7

Find add inverse of 3

(3 + 4) Mod 7 = 7 Mod 7

= 0 Mod 7

$Z_9 = \{0, 1, 2, 3, \dots 8\}$

5 Mod 9

(5+4) Mod 9

0 Mod 9

$a = 2$

a^{-1} Mod 9

7 is additive inverse

M Division

$\left(\frac{8}{8}\right) = \frac{a}{a^{-1}} = 8 \times \frac{1}{8} = 1$

$\downarrow$

Multiplicative inverse of number

- Whenever any number n is multiplied by multiplicative inverse of n then we will get 1 which is multiplicative identity

To do modular division, we req multiplicative inverse
• Because with integer we can't have fractional value
Modular Multiplicative Inverse

$Z_6 = \{0, 1, 2, \cdots 5\}$

GCD = HCF

10: 1, 2, 5, 10

20: 1, 2, 4, 5, 10, 20

common Divisor = 1, 2, 5, 10
GCD = 10

$a \in Z_6 = \{\cancel{0}, \cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, 5\}$

a^{-1} Mod exist iff $GCD(a,b) = 1$

only 5^{-1} Mod 6 exist

$Z_5 = \{\cancel{0}, \cancel{1}, 2, 3, 4\}$

$GCD = \{2, n\}$

2^{-1} Mod 5 exist

3^{-1} Mod 5 exist
Because GCD of $(3, 5) = 1$

4^{-1} Mod 5 exist

$Z_7 = \{0, 1, \ldots 6\}$

DIY

$Z_8 = \{\cancel{0}, \cancel{1}, 2, 3 \ldots 7\}$

$2^{-1} \text{ Mod } 7$

let Z_n

If $n =$ even then only last term

If $n =$ odd than mostly except 0, 1