DMS

Modular Arithmetic

(+, −, ×, ÷)

In cryptography:

Congurence → remainder → ≡

Example:

$19 \equiv 1 \pmod 3$ (1 is the remainder)

$4 \equiv 1 \pmod 3$

$11 \equiv 1 \pmod 3$

$3 \overline{)19}\ 6$, 18, $1 \equiv$

$\Rightarrow$ 1:. $a \equiv b \pmod m$

2:. $a = km + b$

$m \overline{)a}\ k$, b

Valid & invalid Congurence

$19 \equiv 1 \pmod 3$ valid

$10 \equiv 2 \pmod 6$ invalid

$2 \equiv -3 \pmod 5$ valid

$5 \overline{)2}$, 5, -3

:.

O Mod 2 → even

Z = Set of remainders

Z mode 2

$Z_2 = \{0, 1\}$ Class of integers

↓ Infinite members

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

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

$Z_n = \{0, 1, 2, 3, \cdots n-1\}$

n classes

Z mode n : iss main n numbers hain from 0 to $n-1$

⇒ **Arithmetic Addition**

Let

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

∴ by adding any two numbers from Z_5 set we get a single number from this set Z_5.

Example:

addition of 3 & 4

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

addition of 3 & 4 is:

$3 \bmod 5 + 4 \bmod 5$

$(3+4) \bmod 5$

$7 \bmod 5$

$7 \equiv 2 \pmod 5$

$5 \overline{)\,7}$

5

$\overline{2}$

2 is the member of Z_5 set.

Example no 2:

addition of more nbrs

Let

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

by adding 2, 3, 4

$2 \bmod 5 + 3 \bmod 5 + 4 \bmod 5$

$(2+3+4) \bmod 5$

$9 \bmod 5$

$9 \equiv 4 \pmod 5$

$5 \overline{)\,9}$
$\quad 5$
$\quad \overline{4}$

4 is the part of given set

Conclusion

Modular addition is closed.

⇒ **Modular Subtraction:**

i.e. by subtracting any two or more numbers from given set we get a single member from given set.

Mon Tue Wed Thu Fri Sat

(Short Q: Closen property)

Example: 1

two nbr Subtraction.

let

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

3, 6

$3 \bmod 7 - 6 \bmod 7$

$(3-6) \bmod 7$

$-3 \bmod 7$

$-3 \equiv 4 \pmod 7$

$7 \overline{)-3}$

$\frac{7}{4}$

4 is the part of given set.

Example 2:

2, 6

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

$2 \bmod 7 - 6 \bmod 7$

$(2-6) \bmod 7$

$-4 \bmod 7$

$-4 \equiv 3 \pmod 7$

$7 \overline{)-4}$

$\frac{7}{3}$

(3 is part of given set)

Example 3:

more nbrs

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

4, 5, 6

$4 \bmod 7 - 5 \bmod 7 - 6 \bmod 7$

$(4 - 5 - 6) \bmod 7$

$-7 \bmod 7$

$7 \overline{)-7}$

7

0

(0 is the part of given set)

Conclusion:

Modular subtraction is closed.

$\Rightarrow$

Modular Multiplication

Let

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

Example: 1

4, 5

$4 \bmod 7 \times 5 \bmod 7$

$(4 \times 5) \bmod 7$

$20 \bmod 7$

$7 \overline{)20}$ quotient 2, 14, remainder 6

$20 \equiv 6 \pmod 7$

6 → member

Example:2

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

$5 \bmod 7 \times 6 \bmod 7$

$(5 \times 6) \bmod 7$

$30 \bmod 7$

$$7 \overline{)\,30} \quad 4, \text{ remainder } 2$$

$30 \equiv 2 \pmod 7$

(Closed)

Example No 3

mod nbr

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

4, 5, 6

$4 \bmod 7 \times 5 \bmod 7 \times 6 \bmod 7$

$(4 \times 5 \times 6) \bmod 7$

$120 \bmod 7$

$$7 \overline{)\,120} \quad 17, \text{ remainder } 1$$

(Closed)

Conclusion:

Modular Multiplication is Closed.

Imp:

Class → remainder → Smaller + non-negative

Example:

modular Subtraction

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

2, 4

$2 \bmod 7 - 4 \bmod 7$

$(2-4) \bmod 7$

$-2 \bmod 7$

$-2 \equiv 5 \pmod 7$

$7 \overline{)\,-2}$, $\frac{7}{5}$

∴ we want to calculate diff so don't change sign.

(Example 2)

$-22 \bmod 7$

$7 \overline{)\,-22}$, $\frac{21}{-1}$ (wrong)

$7 \overline{)\,-22}$, $\frac{28}{6}$ ✓

(we want non-negative integer)

Encryption of words: Cryptography

∴

In alphabets we have 26 characters so we do all our

our operations in this set.

we set a key to encrypt or decrypt the message.

Example:

CAT

Key = 9

$Z_{26} = \{0, 1, 2, 3, \cdots 25\}$

C A T

$x_1 = 2 \quad x_2 = 0 \quad x_3 = 19$

$y_1 = (x_1 + k) \bmod 26$

$(2 + 9) \bmod 26$

$11 \bmod 26$

$11 = L$

$y_2 = (x_2 + k) \bmod 26$

$(0 + 9) \bmod 26$

$9 \bmod 26$

J

$y_3 = (x_3 + k) \bmod 26$

$(19 + 9) \bmod 26$

$28 \bmod 26$

$28 \equiv 2 \pmod{26}$

$26 \overline{)28}$ 26 2

C

Encrypted message:

LJC

Decryption of message:

$Z_{26} = \{0, 1, 2, 3, \ldots 25\}$

L J C

$y_1 = 11$ $y_2 = 9$ $y_3 = 2$

$k = 9$

$x_1 = (y_1 - k) \bmod 26$

$(11-9) \bmod 26$

$2 \bmod 26$

$= C$

$x_2 = (y_2 - k) \bmod 26$

$(9-9) \bmod 26$

$0 \bmod 26$

A

$x_3 = (y_3 - k) \bmod 26$ (non-negative integers)

$(2-9) \bmod 26$

$-7 \bmod 26$

$26 \overline{)-7}$

$\frac{26}{19}$

$-7 \equiv 19 \pmod{26}$

$19 = T$

Modular Division

aditive identity inverse $= 0$

Multiplicative identity inverse $= 1$

To find aditive inverse

2 aditive 2 mod 7

$(2+5) \bmod 7$

$7 \bmod 7$ } equal

$0 \bmod 7$ }

integer ma jab aditive inverse add karty hy to aditive identity ana chahiye

Example:

aditive inverse of 3?

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

$= (3 + \underset{\downarrow}{4}) \bmod 7$

aditive inverse

$= 7 \bmod 7 \Rightarrow 0 \bmod 7$

Example:

aditive inverse of 6?

$Z_9 = \{0, 1, 2, 3, 4, \cdots 8\}$

$6 \bmod 9$

$(6+3) \bmod 9$ $\quad \therefore 3$ aditive identity

$9 \bmod 9 = 0 \bmod 9$

Division → as Multiplication

Example

$$\frac{8}{8} \Rightarrow 8 \cdot \frac{1}{8} \Rightarrow 8\,\underbrace{8^{-1}}_{\text{Multiplicative inverse}}$$

⇒ To do modular division we required multiplicative inverse

Multiplicative inverse:

⇒ in some cases Z_n has no multiplicative inverse.

GCD: Greatest Common divisor

⇒ if GCD = 1 then inverse is exist otherwise not.

Example:

Mon Tue Wed Thu Fri Sat

(0, 1 ko check ni karna)

$Z_6 = \{0^{\times}, 1^{\times}, 2^{\times}, 3^{\times}, 4^{\times}, 5^{\checkmark}, 6\}$

GCD=2 $2^{-1} \bmod 6$ is not exist ∵ 2(1,2), 6(1,2,3,6) (Divisor, Divisor)

GCD=3 $3^{-1} \bmod 6$ is not exist ∵ 3(1,3), 6(1,2,3,6)

GCD=2 $4 \bmod 6$ is not exist ∵ 4(1,2,4), 6(1,2,3,6)

GCD=1 $5 \bmod 6$ is exist ∵ 5(1,5), 6(1,2,3,6)

Imp: if there is prime number then Multiplicative inverse is exist.
otherwise may or may not be.

Invertible: inverse exist

non-invertible: Inverse not exist

Relatively prime

Two integers (a, b) relativly prime iff GCD (a, b) = 1

∴ $(5, 6)^{\bmod}$ ⇒ is exist because GCD = 1

⇒ prime nbr must have two divisor

⇒ In relative prime, (Compose)

Alternative method to find Multiplicative inverse:

Example: 1

(85, 34)

∴ Compare karna jo bara wali value ho gi usa left side pr likhna aur choti ko right side pr. phir right side pr changing kr k usa left ka equal karna us time tak Solve karna jab tak last pr zero ni ah jata

85 = 34

Step1: 85 = 34(2) + 17

Step2: 34 = 17(2) + 0

17 GCD

Example: 2

1331, 1001

1331 = (1001)(1) + 330

1001 = 330(3) + 11

Example: 3

9888 , 6060

$9888 = (6060)1 + 3828$

$6060 = 3828(1) + 2232$

$3828 = 2232(1) + 1596$

$2232 = 1596(1) + 636$

$1596 = 636(2) + 324$

$636 = 324(1) + 312$

$324 = 312(1) + 12$

$312 = 12(26) + 0$

12 GCD

---

part of Example NO 2

$x = y = ?$

(Smallest value ko break karna)

$1331x + 1001y = 11$

$11 = 1001 - 330(3)$

$1001 - [1331 - 1001][3]$

$1001 - 1331(3) + 1001(3)$

$1001(4) - 1331(3)$

$x = 4, \quad y = 3$

Example: 4

213, 117

$213 = 117(1) + 96$ → 5th

$117 = 96(1) + 21$ → 4th

$96 = 21(4) + 12$ → 3rd

$21 = 12(1) + 9$ → 2nd

$12 = 9(1) + 3$ → 1st

$9 = 3(3) + 0$

3 GCD

To find values

$213x + 117y = 3$

∴ Sab sa choty integer ko break karna

1st $3 = 12 - 9$

(Step 2) 9 ko break karna

$3 = 12 - [21 - 21]$

$12 - 21 + 21$

$3 = 12(2) - 21$

(Step 3)

$3 = [96 - 21(4)](2) - 21$

$= 96(2) - 21(8) - 21$

$= 96(2) - 21(9)$

(Step 4)

$= 96(2) - [117 - 96]9$

$= 96(2) - 117(9) + 96(9)$

$3 = 96(11) - 117(9)$

(Step 5)

$3 = [213 - 117](11) - 117(9)$

$= 213(11) - 117(11) - 117(9)$

$= 213(11) - 117(20)$

$= 213(11) + 117(-20)$

$x = 11 \quad , \quad y = -20$

Example 5:

(252 , 198)

$252 = 198(1) + 54$ ∴ 3rd

$198 = 54(3) + 36$ ∴ 2nd

$54 = 36(1) + 18$ ∴ 1st

$36 = 18(2) + 0$

18 GCD

Mon Tue Wed Thu Fri Sat

$$252x + 198y = 18$$

$$18 = 54 - 36 \quad \text{1st}$$

$$= 54 - [198 - 54(3)] \quad \text{2nd}$$

$$= 54 - 198 + 54(3)$$

$$= 54(4) - 198$$

$$= [252 - 198]5 - 198 \quad \text{3rd}$$

$$= 252(5) - 198(5) - 198$$

$$= 252(5) - 198(6)$$

$$= 252(5) + 198(-6)$$

$$x = 5, \quad y = -6$$