Homework Number : 03
Name : Samitha Ranasinghe
ECN Login : sranasi
Due Date : 01/26/2023

Theory Problems

1) $Z_{18} = \{0, 1, \ldots, 16, 17\}$

With additive operator:

Closure property exists – $a \bmod 18 + b \bmod 18 = c \bmod 18$

Associativity property exists – $(a \bmod 18 + b \bmod 18) + c \bmod 18$
$= a \bmod 18 + (b \bmod 18 + c \bmod 18)$

Identity element – Indentity element which is zero for additive operator exists
$a \bmod 18 + 0 \bmod 18 = a \bmod 18$

Inverse element – For every element, there exists an additive inverse
$a \bmod 18 + b \bmod 18 = 0$

$\therefore Z_{18}$ forms a group with addition operator

With multiplication operator:

Inverse element - Since 18 is not a prime number, not all elements have a multiplicative inverse.

$\therefore$ Z_{18} doesn't form a group with the modulo multiplication operator.

2) gcd(·) for any two numbers will not give 0 as division by 0 is undefined.

$$\gcd(a,b) \neq 0$$

Since it doesn't satisfy the inverse property, W doesn't form a group under gcd(·)

3) $\gcd(10946, 19838)$

$= \gcd(19838, 10946)$
$= \gcd(10946, 8892)$
$= \gcd(8892, 2054)$
$= \gcd(2054, 676)$
$= \gcd(676, 26)$
$= \gcd(26, 0)$

$\therefore \gcd(10946, 19838) = 26$ //

4) MI of 19 in $\mathbb{Z}_{35}$

$\gcd(19, 35)$

$= \gcd(35, 19)$ residue $19 = 1 \times 19 + 0 \times 35$

$= \gcd(19, 16)$ residue $16 = -1 \times 19 + 1 \times 35$

$= \gcd(16, 3)$ reside $3 = 1 \times 19 - 1 \times 16$

$3 = 1 \times 19 - 1 \times (-1 \times 19 + 1 \times 35)$

$3 = 2 \times 19 - 1 \times 35$

$= \gcd(3, 1)$ residue $1 = 1 \times 16 - 5 \times 3$

$1 = (-1 \times 19 + 1 \times 35) - 5(2 \times 19 - 1 \times 35)$

$1 = -11 \times 19 + 6 \times 35$

$-11 \rightarrow 24$ in $\mathbb{Z}_{35}$

$1 \bmod 35 = 24 \times 19 \bmod 35$

$\therefore$ 24 is the MI of 19

5) a) $6x \bmod 23 = 3 \bmod 23$

$$x = \frac{3 \bmod 23}{6 \bmod 23}$$

$x = 3 \bmod 23 \times MI(6)$

Obtain MI of 6 from extended euclid's algorithm, which results in 4.

$x = 3 \times 4$

$x = 12$ //

b) $7x \bmod 13 = 11 \bmod 13$

$$x = \frac{11 \bmod 13}{7 \bmod 13}$$

$x = 11 \times MI(7)$

$x = 11 \times 2 = 22$

$x = 22 \% 13 = 9$ //

c) $5x \bmod 11 = 7 \bmod 11$

$$x = \frac{7 \bmod 11}{5 \bmod 11}$$

$x = 7 \times MI(5)$

$x = 7 \times 9 = 63$

$x = 63 \% 11 = 8$ //