Theory Problems.

ECE Homework 3 - 404 (Question 1)

(Q1) The set of remainders $Z_{18} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}$.

To form a group you must satisfy 4 properties :

1) Associativity
2) Closure
3) Existence of identity element
4) Existence of inverse element.

1) Demonstrate closure : (Addition)

Eg, ~~1 mod 18 = 1~~ No modulo operation can return a value that is ~~2 mod 18 = 2~~ greater than 20, or less than 0.

For eg,

1 mod 20 = 1   2 mod 20 = 2   . . . .   21 mod 20 = 1 . . . 39 mod 20 = 19

Therefore, this group has closure.

2) Associativity (Addition)

Eg, $[20 + (1+4)] \bmod 15 = 10$ $[(20+1)+4] \bmod 15 = 10$

3) Group Identity Element

$(6+0) \bmod 20 = 6$ $6 \bmod 20 = 6$ ✓

$(21+0) \bmod 20 = 1$ $21 \bmod 20 = 1$ ✓

4) Inverse using the identity element.

$(1+19) \bmod 20 = 0$ . . . . $(10+10) \bmod 20 = 0$

$(2+18) \bmod 20 = 0$

∴ We can conclude that Z_n is a group w.r.t the addition operator.

→ However, Z_n is NOT a group w.r.t the multiplication operator. This is because there is no multiplicative inverse for every element in Z_n. Only those that are relatively prime would be a group, since they have a MI.

(Q2) No, the set of all unsigned integers W is not a group because it does not satisfy the 4 properties of being a group.

1) Associativity
$gcd(4,5) = gcd(5,4)$ ∴ Associativity is proved.

2) Closure
$gcd(4,5) = x$ we know x is always going to be an integer. Therefore the gcd of (a,b) where a, b are integers will always result in an integer. ∴ Closure is proved.

3) Identity Element.
we know, $gcd(a,0) = a$ ∴ we can conclude that '0' is the identity element.

4) Inverse
→ since '0' is the identity element we can try to find an inverse. However the gcd of $(a,b) \neq 0$.
$gcd(a,b) \neq 0$, therefore $\boxed{\text{no inverse exists}}$ and since this group follows only 3 out of 4 properties it is $\boxed{\text{NOT}}$ a group.

(Q3) $gcd(10946, 19838)$ ∴ The $gcd(10946, 19838) = \boxed{26}$
$= gcd(19838, 10946)$
$= gcd(10946, 8892)$
$= gcd(8892, 2054)$
$= gcd(2054, 676)$
$= gcd(676, 26)$
$= gcd(26, 0)$

(Q4) M.I of 19 in Z_{35}. To compute this we would have to find the gcd of $(19, 35)$

∴ $gcd(19, 35)$
$= gcd(35, 19)$

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

$= \gcd(16, 3) \rightarrow$ residue : $3 = 1 \times 19 - 1 \times 16$

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

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

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

$= 1 \times 16 - 5(2 \times 19 - 1 \times 35)$

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

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

$\therefore$ The multiplicative inverse of 19 in Z_{35} is $\boxed{24}$

$\boxed{35 - 11 = 24}$

(Q5)

(a) $6x \equiv 3 \pmod{23}$

$x \equiv 3 \times \frac{1}{6} \pmod{23}$

multiplicative inverse of $6 = 4$.

$\therefore x \equiv (3 \times 4) \bmod 23 = 12$

$\boxed{x = 12}$

(b)

$7x \equiv 11 \pmod{13}$

$x = 11 \times \left(\frac{1}{7}\right) \bmod 13$

multiplicative inverse of $7 = 2$

$\boxed{x = 9}$

$x = (11 \times 2) \bmod 13$

$= 22 \bmod 13 = 9$

(c) $5x \equiv 7 \pmod{11}$

$x = 7 \times \frac{1}{5} \pmod{11}$

multiplicative inverse of $5 = 9$

$\boxed{x = 8}$

$x = (7 \times 9) \bmod 11$

$= 63 \bmod 11$

$= 63 - 55 = 8$