NAME :- KRUNAL RANK

ROLL NO :- U18CO081

CLASS :- BTECH 4TH YEAR

SEMESTER :- 7

DIVISION :- B

Cryptography & Network Security
Tutorial 5

Ans 1.

i) $12x \equiv 5 \mod 16$; $x \in [0,16) \cap Z$

$12x = 16y + 5$

There is no such possible value of x for which $12x \% 16 = 5$.

Hence, Ans is ϕ.

ii) $10x \equiv 5 \mod 27$ $x \in [0,27) \cap Z$

$10x = 27y + 5$

For $x = 14$, $10x = 140 \% 27 = 5$

Hence, for all numbers $x = [14]_{27}$, the above congruence relation is valid.

Ans 2. For Z_{10}, additive inverses are (1,9), (2,8), (3,7), (4,6), (5,5).

Ans 3. For given group, $\{Z_{10*}, \times\}$, let's find all cyclic subgroups.

For $\langle 1 \rangle$, ~~A = {1}~~, let the group be G_1

1 belongs to G_1.

$1 * 1 = 1$ which already belongs to G_1.

Hence, G_1 is a cyclic subgroup with $\langle 1 \rangle$.

For $\langle 2 \rangle$, let the subgroup be G_2.

$G_2 = \{\{2\}, \times\}$.

$2 \times 2 = 4$. 4 must belong to G_2.

$4 \times 2 = 8$ 8 must belong to G_2

$8 \times 2 = 16 \% 10 = 6$ must belong to G_2

$6 \times 2 = 12 \% 2 = 2$.

Hence, $G_2 = \{\{2, 4, 8, 6\}, \times\}$ is another cyclic subgroup

Similarly, we get,

$\langle 3 \rangle$, 3

$3 \times 3 = 9$

$9 \times 3 = 27 \% 10 = 7$ Hence, $G_3 = \{\{1, 3, 7, 9\}, \times\} = \langle 3 \rangle$

$7 \times 3 = 21 \% 10 = 1$

$1 \times 3 = 3$

$\langle 4 \rangle$, 4

$4 \times 4 = 16 \% 10 = 6$ Hence, $G_4 = \{\{4, 6\}, \times\} = \langle 4 \rangle$

$6 \times 4 = 24 \% 10 = 4$

$\langle 5 \rangle$, 5

$5 \times 5 = 25 \% 10 = 5$ Hence, $G_5 = \{\{5\}, \times\} = \langle 5 \rangle$

$\langle 6 \rangle$, 6

$6 \times 6 = 36 \% 10 = 6$ Hence, $G_6 = \{\{6\}, \times\} = \langle 6 \rangle$

$\langle 7 \rangle$, 7

$7 \times 7 = 49 \% 10 = 9$

$9 \times 7 = 63 \% 10 = 3$ However, it is equal to G_3.

$3 \times 7 = 21 \% 10 = 1$

$1 \times 7 = 7$

$\langle 8 \rangle$, 8

$8 \times 8 = 64 \% 10 = 4$

$4 \times 8 = 32 \% 10 = 2$ However, it is equal to G_2.

$2 \times 8 = 16 \% 10 = 6$

$6 \times 8 = 48 \% 10 = 8$

$\langle 9 \rangle$ 9 Hence, $G_9 = \{\langle 1, 9\rangle, \times\}$.

$9 \times 9 = 81 \% 10 = 1$

$1 \times 9 = \cancel{81}\ 9$.

$\langle 0 \rangle$ 0 Hence, $G_{10} = \{\langle 0 \rangle, \times\}$.

$0 \times 0 = 0$

Hence, there are 8 cyclic subgroups of given group.

Ans 4)

i) Given $G = \langle Z_{11}, + \rangle$

0 is the identity element.

Now, Order of 1 = 11 {Add 1, 11 times to get $11 \% 11 = 0$}

Order of 2 = 11 {Add 2, 11 times to get $22 \% 11 = 0$}

Order of 3 = 11 {Add 3, 11 times to get $33 \% 11 = 0$}

Hence, order of all elements = 11.

ii) Given $G = \langle Z_{11}^*, \times \}$

1 is the identity element.

[2] = 6

[3] = 4

[4] = 3

[5] = 9

[6] = 2

[7] = 8

[8] = 7

[9] = 5

[10] = 10

0 doesn't have an order.

Date ____
Page ____

Ans 5:

i) $12^{-1} \bmod 77 = \cancel{34}\ 45$

ii) $5^{15} \bmod 13 = 8$

iii) $27^{-1} \bmod 41 = \cancel{1}38$

$\cancel{(27^{39} \bmod 41)}$

$\cancel{(39)_{10} = (101001)_2}$

$\cancel{ans = 1}$

$\cancel{y = 32 + 8 + 1}$

$\cancel{a = 27}$