

1. [Marks 10]

Write the inverse y of all elements x in modulo 10. That is $x * y \equiv 1 \pmod{10}$.

x	1	2	3	4	5	6	7	8	9
y	1	—	7	—	—	—	3	—	9

\uparrow
 $\gcd(2, 10) \neq 1$
 \uparrow
 $\gcd(4, 10) \neq 1$
 \uparrow
 $\gcd(5, 10) \neq 1$
 \uparrow
 $\gcd(6, 10) \neq 1$
 \uparrow
 $\gcd(8, 10) \neq 1$

2. [Marks 10]

Solve the equation $x^2 \equiv 3 \pmod{11}$. Find all the solutions.

ANSWER

$x = \pm 5$

$x = \pm 6$

x	x^2	$x^2 \pmod{11}$
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

Solution $x = 5, x = 6$

3. [Marks 20]

Use the Chinese Remainder Theorem to solve the following equations:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{8}$$

$$x \equiv 5 \pmod{9}$$

ANSWER

$$x = 347$$

$$\text{General solution } x = 347 + 360n$$

5, 8, 9 are relatively prime ✓.

$$n = 5 \times 8 \times 9 = 360, \quad M_1 = \frac{360}{5} = 72, \quad M_2 = \frac{360}{8} = 45$$

$$M_3 = \frac{360}{9} = 40$$

$$M_1 y_1 \equiv 1 \pmod{5} \Rightarrow 72 y_1 \equiv 1 \pmod{5} \quad y_1 = 3$$

$$M_2 y_2 \equiv 1 \pmod{8} \Rightarrow 45 y_2 \equiv 1 \pmod{8} \quad y_2 = 5$$

$$M_3 y_3 \equiv 1 \pmod{9} \Rightarrow 40 y_3 \equiv 1 \pmod{9} \quad y_3 = 7$$

$$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \pmod{n}$$

$$= (2 \times 72 \times 3 + 3 \times 45 \times 5 + 5 \times 40 \times 7) \pmod{360}$$

$$= 2507 \pmod{360} = 347$$

$$x = 347$$

$$x = 347 + n(360)$$

4. [Marks 15]

Express the $\gcd(128, 81)$ as a linear combination of 128 and 81.

ANSWER $\gcd(128, 81) = (-31 \times 128) + (49 \times 81)$

$$128 = 1 \times 81 + 47 \rightarrow 47 = 128 - 1 \times 81$$

$$81 = 1 \times 47 + 34 \rightarrow 34 = 81 - 1 \times 47$$

$$47 = 1 \times 34 + 13 \rightarrow 13 = 47 - 1 \times 34$$

$$34 = 2 \times 13 + 8 \rightarrow 8 = 34 - 2 \times 13$$

$$13 = 1 \times 8 + 5 \rightarrow 5 = 13 - 1 \times 8$$

$$8 = 1 \times 5 + 3 \rightarrow 3 = 8 - 1 \times 5$$

$$5 = 1 \times 3 + 2 \rightarrow 2 = 5 - 1 \times 3$$

$$3 = 1 \times 2 + 1 \rightarrow 1 = 3 - 1 \times 2$$

$$2 = 2 \times 1 + 0$$

$$1 = 3 - 1 \times 2 \Rightarrow = 3 - 1 \times (5 - 1 \times 3) \Rightarrow = -1 \times 5 + 2 \times 3$$

$$= -1 \times 5 + 2 \times (8 - 1 \times 5) = 2 \times 8 - 3 \times 5 = 2 \times 8 - 3(13 - 1 \times 8)$$

$$= -3 \times 13 + 5 \times 8 = -3 \times 13 + 5 \times (34 - 2 \times 13) = 5 \times 34 - 13 \times 13$$

$$= 5 \times 34 - 13 \times (47 - 1 \times 34) = -13 \times 47 + 18 \times 34 = -13 \times 47 + 18(81 - 1 \times 47)$$

$$= 18 \times 81 - 31 \times 47 = 18 \times 81 - 31(128 - 1 \times 81)$$

$$= (-31 \times 128) + (49 \times 81)$$