U20CS005

PAGE NO.
DATE / /

Tutorial-3

1. Find Euler's ~~Rht~~ Totient function for the following:

1) $\phi(29)$ 2) $\phi(80)$

3) $\phi(100)$ 4) $\phi(101)$.

→ 1) $\phi(29)$

Here $n = 29$

n is a prime number

$\phi(n) = n - 1$

$\phi(29) = 28.$

2) $\phi(80)$

here $n = 80.$

$n = 16 \times 5 = 2^4 \times 5.$

Distinct prime factors are 2 & 5

$$\phi(n) = n \times \left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)$$

$$\phi(80) = 80\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 80 \times \frac{1}{2} \times \frac{\cancel{4}\,2}{5}$$

$\phi(80) = 32.$

3) $\phi(100)$

here $n = 100$

$n = 25 \times 4 = 5^2 \times 2^2$

Distinct prime factors are 2 and 5

$$\phi(n) = n \times \left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)$$

$$\phi(100) = 100 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

$$= \overset{20}{\cancel{100}} \times \frac{1}{2} \times \frac{\cancel{4}\,2}{\cancel{5}}$$

$\phi(100) = 40.$

PAGE NO.
DATE / /

4) $\phi(101)$

here $n=101$

n is a prime number

$\phi(n) = n-1 \Rightarrow \phi(101) = 100$

2. Find the value of x for the following set of congruence using chinese remainder theorem.

a) $x \equiv 2 \bmod 7$ & $x \equiv 3 \bmod 9$

b) $x \equiv 4 \bmod 5$ & $x \equiv 10 \bmod 11$

→ a) $x \equiv 2 \bmod 7$ & $x \equiv 3 \bmod 9$

$a_1 = 2,\ a_2 = 3,\ m_1 = 7,\ m_2 = 9.$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M.$

$M = m_1 m_2 = 63.$

$M_1 = \frac{M}{M_1} = \frac{63}{7} = 9$; $M_2 = \frac{M}{m_2} = \frac{63}{9} = 7$

$M_1 M_1^{-1} = 1 \bmod m_1$

$9 M_1^{-1} = 1 \bmod 7.$

$M_1^{-1} = 9^{-1} \bmod 7.$

Q	A	B	R	T_1	T_2	T
0	7	9	7	0	1	0
1	9	7	2	1	0	1
3	7	2	1	0	1	-3.
2	2	1	0	1	-3	7.
	1	0		-3	7	

$\Rightarrow M_1^{-1} = -3 \bmod 7$

$M_1^{-1} = 4$

$M_2 M_2^{-1} = 1 \bmod m_2$

$7 M_2^{-1} = 1 \bmod 9$

$M_2^{-1} = 7^{-1} \bmod 9.$

Q	A	B	R	T_1	T_2	T
1	9	7	2	0	1	-1
3	7	2	1	1	-1	4
2	2	1	0	-1	4	-9
	1	0		4	-9	

$M_2^{-1} = 4 \bmod 9$

$M_2^{-1} = 4$

$\Rightarrow x = (2 \times 9 \times 4 + 3 \times 7 \times 4) \bmod 63$

$= (72 + 84) \bmod 63.$

$= (72 \bmod 63 + 84 \bmod 63) \bmod 63$

$= (9 + 21) \bmod 63$

$x = 30 \bmod 63$

$\Rightarrow x = 30.$

b) $x \equiv 4 \bmod 4$ & $x \equiv 10 \bmod 11.$

$a_1 = 4,\ a_2 = 10,\ m_1 = 4,\ m_2 = 11$

$M = m_1 m_2 = 44$

$M_1 = \frac{M}{m_1} = \frac{44}{4} = 11$

$M_2 = \frac{M}{m_2} = \frac{44}{11} = 4$

$M_1 M_1^{-1} = 1 \bmod m_1$

$11\, M_1^{-1} = 1 \bmod 4$

$M_1^{-1} = 11^{-1} \bmod 4$

Q	A	B	R	T_1	T_2	T
0	4	11	4	0	1	0
2	11	4	3	1	0	1
1	4	3	1	0	1	-1
3	3	1	0	1	-1	4
	1	0		-1	4	

$M_1^{-1} = -1 \bmod 4 = 3 \bmod 4$

$\Rightarrow M_1^{-1} = 3$

$M_2 M_2^{-1} = 1 \bmod m_2$.

$4 M_2^{-1} = 1 \bmod 11$

$M_2^{-1} = 4^{-1} \bmod 11$

Q	A	B	R	T_1	T_2	T
2	11	4	3	0	1	-2
1	4	3	1	1	-2	3
3	3	1	0	-2	3	-11
	1	0.		3	-1	

$\Rightarrow M_2^{-1} = 3 \bmod 11$

$M_2^{-1} = 3$.

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$= (4 \times 11 \times 3 + 10 \times 4 \times 3) \bmod 44$

$= (132 + 120) \bmod 44$.

$= \cancel{(132 + 110 + 10) \bmod 44}$.

$= (220 + 32) \bmod 44$

$= (220 \bmod 44 + 32 \bmod 44) \bmod 44$

$= (0 + 32) \bmod 44$

$\Rightarrow X = 32$.

3. Find result of following using Fermant's little theorem

a) $5^{-1} \bmod 13$ b) $13^{-1} \bmod 17$

$\longrightarrow$ a) $5^{-1} \bmod 13$

$a^{p-1} \equiv 1 \bmod p$

$\Rightarrow a^{-1} \bmod p \equiv a^{p-2} \bmod p$.

$5^{-1} \bmod 13 \equiv 5^{13-2} \bmod 13$

$= 5^{11} \bmod 13$

$= (25^5 \bmod 13 \times 5 \bmod 13) \bmod 13$

$= (-1^5 \bmod 13 \times 5 \bmod 13) \bmod 13$

$= (-1 \times 5) \bmod 13$

$= -5 \bmod 13$

$\Rightarrow 5^{-1} \bmod 13 \equiv 8 \bmod 13$.

$5^{-1} \bmod 13 = 8$ //

b) $15^{-1} \bmod 17$

$a^{-1} \bmod p \equiv a^{p-2} \bmod p$

$15^{-1} \bmod 17 \equiv 15^{17-2} \bmod 17$

$= 15^{15} \bmod 17.$

$= (-2)^{15} \bmod 17.$

$= (-1)(8)(16)^{3} \bmod 17$

$= ((-1 \bmod 17)(8 \bmod 17)(16^{3} \bmod 17)) \bmod 17$

$= (16 \times 8 \times 16) \bmod 17.$

$15^{-1} \bmod 17 \equiv 8 \bmod 17$

$15^{-1} \bmod 17 = 8$