Tutorial 3

Q1 Find the value of $\phi(29)$, $\phi(80)$, $\phi(100)$, $\phi(1$

Q2 Find the value of X for the following set of congruence using the Chinese remainder theorem.

a) $X \equiv 2 \bmod 7$, and $X \equiv 3 \bmod 9$
b) $X \equiv 4 \bmod 5$, and $X \equiv 10 \bmod 11$

Q3 Find the results of the following, using Fermat's little theorem.

a) $5^{-1} \bmod 13$
b) $15^{-1} \bmod 17$

1) $\phi(29) = (29-1) = 28$

$$\phi(80) = \phi(2 \times 40)$$
$$= \phi(2 \times 2 \times 20)$$
$$= \phi(2 \times 2 \times 2 \times 10)$$
$$= \phi(16 \times 5) = \phi(2^4 \times 5^1)$$
$$= 80 \times \left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{5}\right)$$
$$= \frac{80 \times 15 \times 4}{80}$$
$$= 60$$
$$= 80 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$
$$= 80 \times \frac{1}{2} \times \frac{4}{5}$$
$$= 32$$

$$\phi(100) = \phi(2^2 \times 5^2)$$
$$= 100 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$
$$= 100 \times \frac{1}{2} \times \frac{4}{5}$$
$$= 40$$

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

2)

a) $X = 2 \bmod 7$.
$X = 3 \bmod 9$

$a_1 = 2 \qquad m_1 = 7$
$a_2 = 3 \qquad m_2 = 9$

$M = m_1 \times m_2 = 7 \times 9 = 63$

$M_1 = \frac{M}{m_1} = \frac{63}{7} = 9$

$M_2 = \frac{M}{m_2} = 7$

$M_1 M_1^{-1} = 1 \bmod m_1$
$9 M_1^{-1} = 1 \bmod 7$
$M_1^{-1} = 4$

$M_2 M_2^{-1} = 1 \bmod m_2$
$7 M_2^{-1} = 1 \bmod 9$
$M_2^{-1} = 4$

~~$M_1^{-1} = 1 \bmod m_1 = 9 \bmod 7 = 2$~~
~~$M_2^{-1} = 1 \bmod m_2 = 7 \bmod 9 = 7$~~

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$$
$$= (2 \times 9 \times 4 + 3 \times 7 \times 4) \bmod 63$$
$$= (72 + 84) \bmod 63$$
~~$= 183 \bmod 63$~~
~~$= 57$~~
$$= 156 \bmod 63$$
$$= \underline{30}$$

b) $x = 4 \mod 5$

$x = 10 \mod 11$

$a_1 = 4 \qquad m_1 = 5$

$a_2 = 10 \qquad m_2 = 11$

$M = m_1 \times m_2 = 55$

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

$M_2 = 5$

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

$11 \; M_1^{-1} = 1 \mod 5$

$M_1^{-1} = 1$

$M_2 \; M_2^{-1} = 1 \mod m_2$

$5 \; M_2^{-1} = 1 \mod 11$

$M_2^{-1} = 9$

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

$= (4 \times 11 \times 1 + 10 \times 5 \times 9) \mod 55$

$= (44 + 450) \mod 55$

$= 494 \mod 55$

$= \underline{\underline{54}}$

3)

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

p = prime , a = +ve integer not divisible by p

$\Rightarrow a^{p-1} = 1 \bmod p$

$a = 5 \qquad p - 1 =$

$$a^{-1} \bmod p = a^{p-2} \bmod p$$
$$= 5^{13-2} \bmod 13$$
$$= 5^{11} \bmod 13$$
$$= 5 \times 5^{10} \bmod 13$$
$$= 5 \times 25^{5} \bmod 13$$
$$= 5 \times (26-1)^{5} \bmod 13$$
$$= [5 \times {}^5C_0\, 26^5 (-1)^0 + {}^5C_1\, 26^4 (-1)^1 + \ldots {}^5C_5\, 26^0 (-1)^5] \bmod 13$$
$$= [13I + 5 \times (-1)^5] \bmod 13$$
$$= (13I - 5) \bmod 13$$
$$= \underline{8}$$

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

$$a^{-1} \bmod p = a^{p-2} \bmod p$$
$$= 15^{17-2} \bmod 17$$
$$= 15^{15} \bmod 17$$
$$= (-2)^{15} \bmod 17$$
$$= (-2)(2^4)^3 \times 2^2 \bmod 17$$