CNS

ASSIGNMENT 2

1. solution :

$a = 7 \quad ; \quad p = 19$

$a^{p-1} = 1 \pmod{p}$

$7^{19-1} = 1 \pmod{19}$

$7^{18} = 1 \pmod{19}$

$1628413597910449 = 1 \pmod{19}$

$1628413597910449 \ \% \ 19 = 1$

$\therefore$ Fermat's rule is true for given.

2. solution :

$6^{24} \bmod 35$

$= [a^1 \times a^2 \times a^4 \times a^8 \times a^{16} \times \ldots \bmod n]$

$= 6^1 \times 6^2 \times 6^4 \times 6^8 \times a^{16} \times \ldots \bmod 35$

$= 6^{12} \times 6^{12} \bmod 35$

$= (2176782336 \times 2176782336) \bmod 35$

$= 1$

$\therefore 6^{24} \bmod 35 = 1$

3. Solution :

Let x be the moderate

$x \equiv 4 \pmod 5$ → ①

$x \equiv 6 \pmod 8$ → ②

$x \equiv 8 \pmod 9$ → ③

From eqn ①, we get

$x = 4 + 5a$

$4 + 5a \equiv 6 \pmod 8$ [Equating eqn ②]

~~5a = 6 mod~~

$5a \equiv 6 - 4 \pmod 8$

$5a \equiv 2 \pmod 8$

$5 \times 5a \equiv 5 \times 2 \pmod 8$

$25a \equiv 10 \pmod 8$

$\therefore a \equiv 2 \pmod 8$

Substitute a in ①

$x = 4 + 5(2 + 8b)$

$x = 14 + 40b$

Substitute x, a in eqn ③

$14 + 40b \equiv 8 \pmod 9$

$40b \equiv -6 \pmod 9$

$4b \equiv 3 \pmod 9$

$7 \times 4b \equiv 7 \times 3 \pmod 9$

$28b \equiv 21 \pmod 9$

$b \equiv 3 \pmod 9$

$\therefore b = 3 + 9c$

$x = 14 + 40(3 + 9c)$

$x = 134 + 360c$

The smallest positive value of x is obtained by setting $c = 0$, which gives $x = 134$.

4. Solution :

$n - 1 = 2^k \times m$

$341 - 1 = 2^k \times m$

$340 = 2^k \times m$

$\frac{340}{2^k} = m$

$\frac{340}{2^1} = 170$; $\frac{340}{2^2} = 85$; $\frac{340}{2^3} = 42.5$

$k = 2$; $m = 85$

$b_0 = a^m \pmod{n}$

$= 2^{85} \pmod{341}$

$b_0 = 1$

$\therefore$ 341 is a composite number.

5. Solution :

$x = 3 \pmod{4}$

$x = 1 \pmod{5}$

$x = 2 \pmod{3}$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$a_1 = 3 \quad ; \quad a_2 = 1 \quad ; \quad a_3 = 2$

$m_1 = 4 \quad ; \quad m_2 = 5 \quad ; \quad m_3 = 3$

To find :

$M = m_1 \times m_2 \times m_3$

$= 4 \times 5 \times 3$

$M = 60$

$M_1 = \frac{M}{m_1} \qquad M_2 = \frac{M}{m_2} \qquad M_3 = \frac{60}{3}$

$= \frac{60}{4} \qquad = \frac{60}{5} \qquad = 20$

$= 15 \qquad = 12$

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

$15 \times M_1^{-1} = 1 \bmod 4$

$15 \times 3 = 1 \bmod 4$

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

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

$12 \times M_2^{-1} = 1 \bmod 5$

$12 \times 2 = 1 \bmod 5$

$\therefore M_2^{-1} = 2$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$20 \times M_3^{-1} = 1 \bmod 3$

$20 \times \quad = 1 \bmod 3$

$\therefore M_3^{-1} = 2$

$$x = (3 \times 15 \times 3 + 1 \times 12 \times 2 + 2 \times 20 \times 2) \bmod 60$$

$$= (135 + 24 + 80) \bmod 60$$

$$= 239 \bmod 60$$

$$x = 59$$