Home Work N 20

N3.

Find inverse of $4x \equiv 1 \pmod 9$

$4 \cdot 1 \equiv 4 \equiv 4 \pmod 9$

$4 \cdot 2 = 8 \equiv 8 \pmod 9$

$4 \cdot 3 = 12 \equiv 3 \pmod 9$

$4 \cdot 4 = 16 \equiv 7 \pmod 9$

$4 \cdot 5 = 20 \equiv 2 \pmod 9$

$4 \cdot 6 = 24 \equiv 6 \pmod 9$

$4 \cdot 7 = 28 \equiv 1 \pmod 9$

Inverse of 4 mod 9 is 7.

N5.

$a = 4, m = 9$

$sa + tm = \gcd(a, m) = 1$

$4s + 9t = \gcd(4, 9) = 1$

$2 \cdot 4 + 1 = 9$

$1 = 9 - 2 \cdot 4 \Rightarrow 1 = (-2) \cdot 4 + 1 \cdot 9$

$s = -2, t = 1$

$-2 \equiv 7 \pmod 9$

Inverse of 4 mod 9 is 7.

N9.

Find congruence of $4x \equiv 5 \pmod 9$

$4x \equiv 1 \pmod 9 \to 7$

$4x \equiv 5 \pmod 9 \cdot 7$

$28x \equiv 35 \pmod 9$

$1x \equiv 8 \pmod 9$

$x = 8 \pmod 9$

Congruence of $4x \equiv 5 \pmod 9$ is 8. $\rightarrow 4 \cdot 8 \equiv 5 \pmod 9$

N20

$x = a_1 \pmod{m_1} \rightarrow x = 2 \pmod 3$

$x = a_2 \pmod{m_2} \rightarrow x = 1 \pmod 4$

$x = a_3 \pmod{m_3} \rightarrow x = 3 \pmod 5$

$M = 3 \cdot 4 \cdot 5 = 60$

$M_1 = 60/3 = 20$

$M_2 = 60/4 = 15$

$M_3 = 60/5 = 12$

$y_1 = 20 \equiv 1 \pmod 3 = 5$

$y_2 = 15 \equiv 1 \pmod 4 = 3$

$y_3 = 12 \equiv 1 \pmod 5 = 3$

$x = (2 \cdot 20 \cdot 5) + (1 \cdot 15 \cdot 3) + (3 \cdot 12 \cdot 3) = 200 + 45 +$

$+ 108 = 353 \pmod{60} \rightarrow 60 \cdot 5 + 53 = 353$

$x = 53 \pmod{60}$.

N23

1) $x \equiv 2 \pmod 3 \rightarrow x = 3k + 2$

2) $x \equiv 1 \pmod 4 \rightarrow x = 4j + 1$

3) $x \equiv 3 \pmod 5 \rightarrow x = 5l + 3$

$1) \to 2)$

• $3k+2 \equiv 1 \pmod 4$

$\cancel{3}k \equiv -1 \equiv \cancel{3} \pmod 4$

$k \equiv 1 \pmod 4$

$2) \to 1)$

~~4j+1 =~~ • $x = 3k+2$

$x = 3(4j+1)+2 = 12j+3+2 = 12j+5$

$2) \to 3)$

• $12j+5 \equiv 3 \pmod 5$

$\cancel{12}j \equiv -2 \equiv \cancel{3} \pmod 5$

~~4j ≡~~ $2j \equiv 3 \pmod 5$

$3(2j) \equiv 3 \cdot 3 \pmod 5$

$j \equiv 9 \equiv 4 \pmod 5$

~~2) → 3)~~ $j = 5l+4 \to x = 12j+5$

$x = 12(5l+4)+5 = 60l+48+5 = 60l+53$

$x = 53 \pmod{60}$.

N33

$a^{(p-1)} \equiv 1 \pmod p$

$7^{121} \bmod 13 \longrightarrow 7^{12} \equiv 1 \pmod{13}$

$121 \mid 12 = 10 \cdot 12 + 1$

$7^{121} = 7^{(10 \cdot 12+1)} = (7^{12})^{10} \cdot 7^1 = 1^{10} \cdot 7^1 = 1 \cdot 7 = 7 \equiv 7$
$\pmod{13}$

$7^{121} \pmod{13} = 7$.