

Home Work N 20

N 3.

Find inverse of  $\forall 4x \equiv 1 \pmod{9}$

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

$$4 \cdot 2 \equiv 8 \equiv 8 \pmod{9}$$

$$4 \cdot 3 \equiv 12 \equiv 3 \pmod{9}$$

$$4 \cdot 4 \equiv 16 \equiv 7 \pmod{9}$$

$$4 \cdot 5 \equiv 20 \equiv 2 \pmod{9}$$

$$4 \cdot 6 \equiv 24 \equiv 6 \pmod{9}$$

$$4 \cdot 7 \equiv 28 \equiv 1 \pmod{9}$$

Inverse of 4 mod 9 is 7.

N 5.

$$a = 4, m = 9$$

$$8a + tm = \text{gcd}(a, m) = 1$$

$$48 + 9t = \text{gcd}(4, 9) = 1$$

$$2 \cdot 4 \neq 1 = 9$$

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

$$3 = -2, t = 1$$

$$-2 \equiv 7 \pmod{9}$$

Inverse of 4 mod 9 is 7.

N 9.

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

$$4x \equiv 1 \pmod{9} \rightarrow \cancel{4} \cdot 1$$

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

$$28x \equiv 35 \pmod{9}$$

$$1x \equiv 8 \pmod{9}$$

$$x \equiv 8 \pmod{9}$$

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

N<sub>20</sub>

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

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

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

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

$$M_1 = 60/3 = 20$$

$$M_2 = 60/4 = 15$$

$$M_3 = 60/5 = 12$$

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

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

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

$$x = (2 \cdot 20 \cdot 5) + (4 \cdot 15 \cdot 3) + (3 \cdot 12 \cdot 5) = 200 + 180 + 180 + 108 = 553 \pmod{60}$$

$$+ 108 = 553 \pmod{60} \rightarrow 60 \cdot 5 + 53 = 353$$

$$x = 53 \pmod{60}$$

N<sub>23</sub>

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

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

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

$$\begin{aligned} 1) &\rightarrow 2) \\ 3k + 2 &\equiv 1 \pmod{4} \\ 3k &\equiv -1 \equiv 3 \pmod{4} \\ k &\equiv 3 \pmod{4} \end{aligned}$$

$$2) \rightarrow 1) \\ \cancel{4j + 1} \equiv \cancel{3} \pmod{4}$$

$$x = 3(4j + 1)$$

$$2) \rightarrow 3)$$

$$12j + 5 \equiv 3 \pmod{4}$$

$$12j \equiv -2 \equiv 2 \pmod{4}$$

$$3(2j) = 3 \pmod{4}$$

$$j \equiv 1 \equiv 9 \pmod{8}$$

$$2) \rightarrow 3)$$

$$x = 12(5j + 1)$$

$$x = 53 \pmod{60}$$

N<sub>33</sub>

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

$$7^{121} \pmod{12}$$

$$121 \mid 12 = 10 \dots 1$$

$$7^{121} \pmod{12}$$

$$(7^4)^{30} \cdot 7 \pmod{12}$$

$$1 \pmod{12}$$

$$1) \rightarrow 2)$$

$$\bullet 3k + 2 \equiv 1 \pmod{4}$$

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

$$k \equiv 3 \pmod{4}$$

$$2) \rightarrow 1)$$

~~$$x = 3(4j+1) + 2$$~~

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

$$2) \rightarrow 3)$$

$$\bullet 12j + 5 \equiv 3 \pmod{5}$$

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

$$4j \equiv 2j \equiv 3 \pmod{5}$$

$$3(2j) = 3 \cdot 3 \pmod{5}$$

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

~~$$2) \rightarrow 3) j = 5l + 4 \Rightarrow x = 12j + 5$$~~

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

$$x = 53 \pmod{60}.$$

45+

N33

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

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

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

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

$$\pmod{13}$$

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