

EGCO 476 – 1<sup>st</sup> Assignment

6213133

Submission – Thu 15<sup>th</sup> Sep 2022

Marking – 10%

Math for Traditional Crypto

30. List all additive inverse pairs in modulus 20.
31. List all multiplicative inverse pairs in modulus 20.
32. Find the multiplicative inverse of each of the following integers in  $\mathbf{Z}_{180}$ 
  - a. 38
  - b. 7
  - c. 132
  - d. 24
36. Find all solutions to each of the following linear equations:
  - a.  $3x \equiv 4 \pmod{5}$
  - b.  $4x \equiv 4 \pmod{6}$
  - c.  $9x \equiv 12 \pmod{7}$
  - d.  $256x \equiv 442 \pmod{60}$

Math for Asymmetrical Crypto

21. Find the results of the following.
  - a.  $5^{15} \pmod{13}$
  - b.  $15^{18} \pmod{17}$
  - c.  $456^{17} \pmod{17}$
  - d.  $145^{102} \pmod{101}$
22. Find the results of the following.
  - a.  $5^{-1} \pmod{13}$
  - b.  $15^{-1} \pmod{17}$
  - c.  $27^{-1} \pmod{41}$
  - d.  $70^{-1} \pmod{101}$

$$30) (0,0), (1,19), (2,18), (3,17) \\ (4,16), (5,15), (6,14), (7,13) \\ (8,12), (9,11), (10,10)$$

$$31) \varphi(20) = \varphi(2^2 \cdot 5) = (2^2 - 2)(5 - 1) = 2 \cdot 4 \\ = 8$$

$$\text{relative prime } 20 = 1, 3, 7, 9, 11, 13, 17, 19$$

$$(1,1), (3,7), (9,9), (11,11)$$

$$(13,17), (19,19)$$

$$32) a. (38, 180) \neq 1 \rightarrow \text{no inverse}$$

$$b. (7, 180) = 1$$

$$c. (132, 180) \neq 1 \rightarrow \text{no inverse}$$

$$d. (29, 180) \neq 1 \rightarrow \text{no inverse}$$

$$\begin{array}{l|l}
 b. \ 7x \equiv 1 \pmod{180} & 180 = 5 \cdot 36 = 5 \cdot 9 \cdot 4 \\
 & = 2^2 \cdot 3^2 \cdot 5 \\
 x = 7^{\varphi(180) - 1} \pmod{180} & \varphi(180) = (2^2 - 2)(3^2 - 3)(5 - 1) \\
 & = (2)(6)(4) = 60 \\
 & = 7^{59} \pmod{180}
 \end{array}$$

$$= 49 \cdot 7^{59} \pmod{180}$$

$$= 49 \cdot (343)^{19} \pmod{180}$$

$$= 49 \cdot (163)^{19} \pmod{180}$$

$$= 7987 \cdot (163)^{19} \pmod{180}$$

$$= 67 \cdot (26567)^9 \pmod{180}$$

$$= 67 \cdot (109)^9 \pmod{180}$$

$$= 7303 \cdot (11491)^4 \pmod{180}$$

$$= 103 \cdot 1^4 \pmod{180}$$

$$= 103$$

$$36) a. \quad 3x \equiv 4 \pmod{5} \quad (3, 4) = 1$$

$$x \equiv 4 \cdot 3^{-1} \pmod{5}$$

$$= 4 \cdot 3^{4(5)-1} \pmod{5}$$

$$= 4 \cdot 3^{(5-1)} \pmod{5}$$

$$= 4 \cdot 3^3 \pmod{5}$$

$$= 4 \cdot 27 \pmod{5}$$

$$= 3$$

~~XXXX~~

$$b. \quad 4x \equiv 4 \pmod{6} \quad (4, 6) = 2 \rightarrow 2 \text{ Answer}$$

$$2x \equiv 2 \pmod{3}$$

$$x \equiv 2 \cdot 2^{-1} \pmod{3}$$

$$= 2 \cdot 2^{3-1-1} \pmod{3}$$

$$= 2 \cdot 2 \pmod{3}$$

$$x = 1$$

$$\therefore x = 1, 4$$

~~XXXX~~

$$c. \quad 9x \equiv 12 \pmod{7} \quad (9, 7) = 1$$

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

$$x \equiv 5 \cdot 9^{-1} \pmod{7}$$

$$\equiv 5 \cdot 9^{7-1-1} \pmod{7}$$

$$\equiv 5 \cdot 9^5 \pmod{7}$$

$$\equiv 5 \cdot 2^5 \pmod{7}$$

$$\equiv 10 \cdot 16 \pmod{7}$$

$$\equiv 3 \cdot 2 \pmod{7}$$

$$x \equiv 6$$

$$d. \quad 256x \equiv 442 \pmod{60} \quad (256, 60) = 4$$

$$4 \nmid 442$$

$\therefore$  no solution

$$\begin{aligned}
 21. a) \quad 5^{15} \bmod 13 &= 5 \cdot 25^7 \bmod 13 \\
 &= 5 \cdot 12^7 \bmod 13 \\
 &= 60 \cdot 12^6 \bmod 13 \\
 &= 60 \cdot 144^3 \bmod 13 \\
 &= 8 \cdot 1^3 \bmod 13 \\
 &= 8
 \end{aligned}$$

$$\begin{aligned}
 b) \quad 5^{18} \bmod 17 &= 25^9 \bmod 17 \\
 &= 8^9 \bmod 17 \\
 &= 2^{27} \bmod 17 \\
 &= 2^2 \cdot (2^5)^5 \bmod 17 \\
 &= 4 \cdot 32^5 \bmod 17 \\
 &= 4 \cdot 15^5 \bmod 17 \\
 &= 60 \cdot 225^2 \bmod 17 \\
 &= 9 \cdot 4^2 \bmod 17 \\
 &= 144 \bmod 17 \\
 &= 8
 \end{aligned}$$

$$\begin{aligned}
 c) \quad 456^{19} \bmod 19 &= 14^{19} \bmod 19 \\
 &= 14 \cdot 14^8 \bmod 19 \\
 &= 14 \cdot 9^9 \bmod 19 \\
 &= 14 \cdot 3^{16} \bmod 19 \\
 &= 42 \cdot 29^5 \bmod 19 \\
 &= 8 \cdot 10^5 \bmod 19 \\
 &= 90 \cdot 100^2 \bmod 19 \\
 &= 12 \cdot 15 \bmod 19 \\
 &= 180 \bmod 19 \\
 &= 10
 \end{aligned}$$

$$\begin{aligned}
 d) \quad 195^{102} \bmod 101 &= 44^{102} \bmod 101 \\
 &= 4^{102} \cdot 11^{102} \bmod 101 \\
 &= 2^{204} \cdot 11^{102} \bmod 101 \\
 &= 2 \cdot (6^7)^{29} \cdot (121)^{51} \bmod 101 \\
 &= 2 \cdot (29)^{29} \cdot 10^{51} \bmod 101 \\
 &= 2 \cdot 3^{97} \cdot 10^{51} \bmod 101 \\
 &= 2 \cdot 3^2 \cdot (3^5)^{17} \cdot (1000)^{17} \bmod 101 \\
 &= 18 \cdot (41)^{17} \cdot 91^{17} \bmod 101
 \end{aligned}$$

$$= 19.41 \cdot 91 \cdot (1681)^8 \cdot (8281)^9 \pmod{101}$$

$$= 67158 \cdot 65^9 \cdot 100^7 \pmod{101}$$

$$= 99 \cdot 65^9 \cdot 10^{14} \pmod{101}$$

$$= 9900 \cdot 4225^4 \cdot 1000^4 \pmod{101}$$

$$= 7 \cdot 84^4 \cdot 91^4 \pmod{101}$$

$$\begin{array}{c} \text{4} \quad \text{21} \quad \text{9} \\ \text{3} \quad \text{7} \quad \text{13} \end{array}$$

$$= (3 \cdot 4 \cdot 9)^4 \cdot 7 \cdot (7 \cdot 13)^4 \pmod{101}$$

$$= 3^9 \cdot 4^9 \cdot 7^9 \cdot 13^4 \pmod{101}$$

$$= 81 \cdot 54 \cdot 40^3 \cdot 69^2 \pmod{101}$$

$$= 4374 \cdot 64000 \cdot 4624 \pmod{101}$$

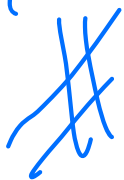
$$= 31 \cdot 67 \cdot 29 \pmod{101}$$

$$= 2077 \cdot 29 \pmod{101}$$

$$= 57 \cdot 79 \pmod{101}$$

$$= 4503 \pmod{101}$$

$$= 59$$





22 .

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

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

$$= 5^{11} \bmod 13$$

$$= 5 \cdot 25^5 \bmod 13$$

$$= 5 \cdot 12^5 \bmod 13$$

$$= 60 \cdot 144^2 \bmod 13$$

$$= 60$$

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

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

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

$$= 15 \cdot 225^9 \bmod 17$$

$$= 15 \cdot 4^9 \bmod 17$$

$$= 60 \cdot 4^6 \bmod 17$$

$$= 60 \cdot 64^2 \bmod 17$$

$$= 9 \cdot 13^2 \bmod 17$$

$$= 9 \cdot 16 \bmod 17$$

$$= 8$$

$$(c) 29^{-1} \bmod 41 = 29^{4(41)-1} \bmod 41$$

$$= 29^{41 \cdot 4 - 1} \bmod 41$$

$$= 29^{39} \bmod 41$$

$$= 3^{117} \bmod 41$$

$$= 3 \cdot 3^{116} \bmod 41$$

$$= 3 \cdot 91^{29} \bmod 41$$

$$= 3 \cdot 40^{29} \bmod 41$$

$$= 3 \cdot 2^{29} \cdot 10^{29} \bmod 41$$

$$= 3 \cdot 2^{98} \cdot 5^{29} \bmod 41$$

$$= 3 \cdot 2^{98} \cdot 125^8 \bmod 41$$

$$= 3 \cdot 2^{98} \cdot 2^8 \bmod 41$$

$$= 3 \cdot 2^{56} \bmod 41$$

$$= 12 \cdot (2^6)^9 \bmod 41$$

$$= 12 \cdot 23^9 \bmod 41$$

$$= 276 \cdot 529^9 \bmod 41$$

$$= 30 \cdot 37^4 \bmod 41$$

$$= 30 \cdot 16^2 \bmod 41$$

$$= 30 \cdot 10 \bmod 41 = 13$$

$$\begin{aligned}
d) \quad 20^{-1} \text{ mod } 101 &= 26^{2(101)-1} \text{ mod } 101 \\
&= 26^{99} \text{ mod } 101 \\
&= 20 \cdot 4900^{99} \text{ mod } 101 \\
&= 20 \cdot 52^{99} \text{ mod } 101 \\
&= 20 \cdot 82^{24} \text{ mod } 101 \\
&= 20 \cdot 58^{12} \text{ mod } 101 \\
&= 20 \cdot 31^6 \text{ mod } 101 \\
&= 20 \cdot 52^3 \text{ mod } 101 \\
&= 3640 \cdot 2204 \text{ mod } 101 \\
&= 4 \cdot 28 \text{ mod } 101 \\
&= 312 \text{ mod } 101 \\
&= 9
\end{aligned}$$
