6213133

EGCO 476 – 1st Assignment

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

30) (0,0), (1,19), (2,18), (3,17)

(4,16), (5,15), (6,14), (7,13)

(8,12), (9,11), (10,10)

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

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) $\neq 1$ → no inverse

b. (7, 180) = 1

c. (132, 180) $\neq 1$ → no inverse

d. (24, 180) $\neq 1$ → no inverse

b. $7x \equiv 1 \bmod 180$

$x = 7^{\varphi(180)-1} \bmod 180$

$180 = 5 \cdot 36 = 5 \cdot 9 \cdot 4$

$= 2^2 \cdot 3^2 \cdot 5$

$\varphi(180) = (2^2-2)(3^2-3)(5-1)$

$= (2)(6)(5) = 60$

$\equiv 7^{59} \bmod 180$

$\equiv 49 \cdot 7^{57} \bmod 180$

$\equiv 49 \cdot (343)^{19} \bmod 180$

$\equiv 49 \cdot (163)^{19} \bmod 180$

$\equiv 7987 \cdot (163)^{18} \bmod 180$

$\equiv 67 \cdot (26569)^9 \bmod 180$

$\equiv 67 \cdot (109)^9 \bmod 180$

$\equiv 7303 \cdot (11881)^4 \bmod 180$

$\equiv 103 \cdot 1^4 \bmod 180$

$\equiv 103$ //

36) a. $3x \equiv 4 \bmod 5 \qquad (3,4)=1$

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

$\equiv 4 \cdot 3^{\phi(5)-1} \bmod 5$

$\equiv 4 \cdot 3^{(5-1)-1} \bmod 5$

$\equiv 4 \cdot 3^{3} \bmod 5$

$\equiv 4 \cdot 27 \bmod 5$

$\equiv 3$

b. $4x \equiv 4 \bmod 6 \qquad (4,6) = 2 \to 2$ Answer

$2x = 2 \bmod 3$

$x = 2 \cdot 2^{-1} \bmod 3$

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

$= 2 \cdot 2 \bmod 3$

$x = 1$

$\therefore \quad x = 1, 4$

c. $9x \equiv 12 \bmod 7 \qquad (9,7) = 1$

$9x \equiv 5 \bmod 7$

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

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

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

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

$\equiv 10 \cdot 16 \bmod 7$

$\equiv 3 \cdot 2 \bmod 7$

$x = 6$ //

d. $256x \equiv 442 \bmod 60 \qquad (256, 60) = 4$

$4 \nmid 442$

$\therefore$ no solution //

21. a) $5^{15} \bmod 13 = 5 \cdot 25^7 \bmod 13$

$= 5 \cdot 12^7 \bmod 13$

$= 60 \cdot 12^6 \bmod 13$

$= 60 \cdot 144^3 \bmod 13$

$= 8 \cdot 1^3 \bmod 13$

$= 8$ //

b) $5^{18} \bmod 17 = 25^9 \bmod 17$

$= 8^9 \bmod 17$

$= 2^{27} \bmod 17$

$= 2^2 \cdot (2^5)^5 \bmod 17$

$= 4 \cdot 32^5 \bmod 17$

$= 4 \cdot 15^5 \bmod 17$

$= 60 \cdot 225^2 \bmod 17$

$= 9 \cdot 4^2 \bmod 17$

$= 144 \bmod 17$

$= 8$ //

c) $456^{17} \bmod 19 = 14^{17} \bmod 19$

$= 14 \cdot 196^{8} \bmod 19$

$= 14 \cdot 9^{8} \bmod 19$

$= 14 \cdot 3^{16} \bmod 19$

$= 42 \cdot 27^{5} \bmod 19$

$= 8 \cdot 10^{5} \bmod 19$

$= 80 \cdot 100^{2} \bmod 19$

$= 12 \cdot 11 \bmod 19$

$= 132 \bmod 19$

$= 10$

d) $495^{102} \bmod 101 = 44^{102} \bmod 101$

$= 4^{102} \cdot 11^{102} \bmod 101$

$= 2^{204} \cdot 11^{102} \bmod 101$

$= 2 \cdot (2^{7})^{29} \cdot (121)^{51} \bmod 101$

$= 2 \cdot (29)^{29} \cdot 20^{51} \bmod 101$

$= 2 \cdot 3^{87} \cdot 20^{51} \bmod 101$

$= 2 \cdot 3^{2} \cdot (3^{5})^{17} \cdot (1000)^{17} \bmod 101$

$= 18 \cdot (41)^{17} \cdot 91^{17} \bmod 101$

$$= 19.41 \cdot 91 \cdot (1681)^8 \cdot (8281)^9 \bmod 101$$

$$= 69158 \cdot 65^9 \cdot 100^7 \bmod 101$$

$$= 94 \cdot 65^9 \cdot 10^{14} \bmod 101$$

$$= 9400 \cdot 6225^4 \cdot 1000^4 \bmod 101$$

$$= 7 \cdot 84^4 \cdot 91^4 \bmod 101$$

$4 \mid 21$, $3 \mid 7$, $13 \mid 91$

$$= (3 \cdot 4 \cdot 7)^4 \cdot 7 \cdot (7 \cdot 13)^4 \bmod 101$$

$$= 3^4 \cdot 4^4 \cdot 7^9 \cdot 13^4 \bmod 101$$

$$= 81 \cdot 54 \cdot 40^3 \cdot 68^2 \bmod 101$$

$$= 4374 \cdot 64000 \cdot 4624 \bmod 101$$

$$= 31 \cdot 67 \cdot 99 \bmod 101$$

$$= 2077 \cdot 99 \bmod 101$$

$$= 57 \cdot 99 \bmod 101$$

$$= 4503 \bmod 101$$

$$= 59$$

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

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

$= 5^{11} \bmod 13$

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

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

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

$= 60 \bmod 13$

$= 8$ ✗

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

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

$= 15^{15} \bmod 17$

$= 15 \cdot 225^7 \bmod 17$

$= 15 \cdot 4^7 \bmod 17$

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

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

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

$= 9 \cdot 16 \bmod 17$

$= 8$ ✗

() $29^{-1} \bmod 91 = 29^{\varphi(91)-1} \bmod 91$

$= 29^{91-1-1} \bmod 91$

$= 29^{89} \bmod 91$

$= 3^{117} \bmod 91$

$= 3 \cdot 3^{116} \bmod 91$

$= 3 \cdot 81^{29} \bmod 91$

$= 3 \cdot 80^{29} \bmod 91$

$= 120 \cdot 1600^{14} \bmod 91$

$= 38 \cdot 1^{14} \bmod 91$

$= 38$

#

d) $20^{-1} \bmod 101 = 20^{\varphi(101)-1} \bmod 101$

$= 20^{99} \bmod 101$

$= 20 \cdot 400^{49} \bmod 101$

$= 20 \cdot 52^{98} \bmod 101$

$= 20 \cdot 2704^{24} \bmod 101$

$= 20 \cdot 74^{24} \bmod 101$

$= 20 \cdot 6084^{12} \bmod 101$

$= 20 \cdot 24^{6} \bmod 101$

$= 20 \cdot 576^{3} \bmod 101$

$= 20 \cdot 71^{3} \bmod 101$

$= 8820 \cdot 5041 \bmod 101$

$= 21 \cdot 92 \bmod 101$

$= 1932 \bmod 101$

$= 13$ //