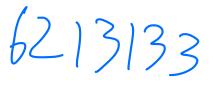
EGCO 476 – 1st Assignment



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} 1
 - 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. 515 mod 13
 - b. 1518 mod 17
 - c. 45617 mod 17
 - d. 145102 mod 101
- 22. Find the results of the following,
 - a. 5-1 mod 13
 - b. 15⁻¹ mod 17
 - c. 27-1 mod 41
 - d. 70⁻¹ mod 101

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

rative prime
$$20 = 13799111 (31719)$$

$$(1317) (919) (1111)$$

$$(1317) (1919)$$

32)
$$a_{1}(39_{1}(80) \neq 1 - 0 \text{ ho inverse}$$
 $b_{1}(7_{1}(90) = 1)$
 $c_{2}(190) \neq 1 - 0 \text{ ho inverse}$
 $d_{1}(29_{1}(90) \neq 1 - 0 \text{ ho inverse}$

b. $7K = 1 \mod 140$ $= 2^{1.3} \cdot 7$ $= 2^{1.3} \cdot 7$ $= 2^{1.3} \cdot 7$ $= (3^{2} - 2)(3^{2} - 3)(5^{-1})$ = 59 modiso = 49. 757 mod 180 = 49. (343) mod 180 = 49. (163) mod 180 = 7997 · (63) nod 180 = 67 · (26,569) modigo = 67. (109) 9 mod140 = 7303. (11 491) 4 mo \$140 = 103 - 14 mod140 = 103

6.
$$QX = 4 \text{ mod } b$$
 $(4,6) = 2 - 0 2 \text{ Answer}$

$$2X = 2 \text{ mod } 3$$

$$X = 2 \cdot 2^{-1} \text{ mod } 3$$

$$= 2 \cdot 2 \text{ mod } 3$$

exqq2 :. ho solution 21.9) fitmod 13 = 5.25 mod 13 = 5. 127 mbd13 = 60-12 mod13 = 60, 1443 mod13 = 8. 13 nol13 b) 5 modi? = 259 modi? = 8º modi9 = 27 ~417 = 2 (25) moli) = 4. 725 mod 17 = 4. 15 mbd19 = 60.227 mode) = 9.42 mod 17 = 144 mod 19

() 476 modes = 1419 modes = (4. 196 modi) = 14. 9 mod19 - 14.3 model7 = 42.79 mod 17 = 9.10 modi9 = 90. (00 modi7 = (2. It modil = 190moles d) 197 madeo = 44 mod 101 = 4 . ((mod (v) = 204 (62 mod 10) = 2-67)29. (121) 1 modes = 2. (29)29. cof model = 2. 3 ?? . (pt rodul = 2.3 - (31) (1000) madiol = 19, (41) ? 21 modial

= (8.41.41. (1881), (8581), moying = 67158 · 659. [607 modeol = 94.679 - 1014 modeol - 4400 - 6552 d. 1000 mogen = 7.84.91 midiol = (3.4.9)4. 7. (7.13) moder = 39.49.99.13 modlo1 = 81 . 54 . 403 .692 mod (0) = 4374.69000.9629 midlel = 31. 67. 29 modial = 2017, 99 noble = 57.72 mallol = 4703 modes)

22. 9) 5-1 modi3 = 56(13)-1 modi3 = 5 mal3 = ~ midiz = 5.25 modi3 = 5. 12 mod 13 = 60. 1992 mid13 _ 60 Hod13 6) 15" md 17 = 15 (M)-1 md17 = (9-1-1 mode) = 15 mod 19 = (r. 217 mol) = 15.49 mode? = 60.4° node9 -60, 692 mondo = 9. 13 not17 = 7. [b modi7

= 8 *

() 29-1 mola(= 29 moda) = 2991-1-1 m/41 = 299 model = 3 60/41 = 3.3 mala1 - 3. 9129 model = 3. 80 mod91 = 120 - 1600 mod91 = 38. 19 mdal = 38

d) 20-(moleo) = 20 (((01)-(moleo) = 90 mod 101 = 70, 4900 marol = 711. 52 modeol -70-2904 nodici = 70, 749 malol = 20 . PO & & Wood [8] 290.24 maliol = 70, 576 nolus = 90. 713 miller = 8790 . 5041 mod vol = 21 - 92 modis/ = 1932 notes = 13