Homework 1 solutions

Total points: 5

---

1 (0.5pt). What integers do the sets Z_{28} and Z_{28*} contain? For each set, list all additive inverse pairs and multiplicative inverse pairs.

Z_{28}= {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27}

Z_{28*} = {1,3,5,9,11,13,15,17,19,23,25,27}

Additive inverse pairs:
(0,0),(1,27),(2,26),(3,25),(4,24),(5,23),(6,22),(7,21),(8,20),(9,19),(10,18), (11,17) ,(12,16),(13,15),(14,14)

Multiplicative inverse pairs:
(1,1),(3,19),(5,17)(13,13)(11,23),(15,15),(25,9),(27,27)

---

2 (1pt). Using extended Euclidean algorithm, show the steps of finding the following multiplicative inverses

a) 321^{-1} mod 56709.

q	r1	r2	r	t1	t2	t
176	56709	321	213	0	1	-176
1	321	213	108	1	-176	177
1	213	108	105	-176	177	-353
1	108	105	3	177	-353	530
35	105	3	0	-353	530	-18903
	3	0		530	-18903	

Gcd(321,56709) != 1, so the multiplicative inverse doesn't exist.

b) 345^{-1} mod 76408

q	r1	r2	r	t1	t2	t
221	76408	345	163	0	1	-221
2	345	163	19	1	-221	443
8	163	19	11	-221	443	-3765
1	19	11	8	443	-3765	4208
1	11	8	3	-3765	4208	-7973
2	8	3	2	4208	-7973	20154
1	3	2	1	-7973	20154	-28127
2	2	1	0	20154	-28127	76408
	1	0		-28127	76408	

Gcd(345,76408) = 1, so 345^{-1} mod 76408 = -28127 mod 76408 = 48218

3(1pt). Find the all solutions to each of the following linear equations

a) 24x ≡ 12 (mod 28)

gcd(24, 28) = 4 and 4 divides 12, so there is 4s olution.

Dividing both sides by 4:

6x ≡ 3 (mod 7)

6^{-1} mod 7 ≡ 6 mod 7

x0 = (3 * 6^{-1})mod 7 =18 mod 7 = 4

x1 = 4+ 1(28/4) = 11

x2 = 4+2(28/4) = 18

x3 = 4+3(28/4) = 25

b) 4x + 5 ≡ 17(mod 10)

à 4x + 5 ≡ 7(mod 10)

à 4x ≡ 2 (mod 10)

Gcd(4,10) = 2, so there are 2 solutions

Divide both sides by 2:

2x ≡ 1 (mod 5)

x0 = 2^{-1} mod 5 = 3

x1 = 3+ (10/2) = 8

c) 5x ≡ 15(mod 25)

gcd(5,25) = 5, 5 divides 15, so there are 5 solutions

divide both sides by 5

x0 = 3(mod 5)

x1 = 3+1(25/5) = 8

x2 = 3+2(25/5) = 13

x3 = 3+3(25/5) = 18

x4 = 3+4(25/5) = 23

d) 24x +20 ≡ 29 (mod 69)

à24x ≡ 9 (mod 69)

Gcd(24,69) = 3, 3 divides 9, so there are 3 solutions.

Divide both sides by 3:

8x ≡ 3 (mod 23)

8^{-1} mod 23 = 3

x0 = 3*8^{-1} mod 23 = 9

x1 = 9+(69/3) = 32

x2 = 9+2(69/3) = 55

---

4 (0.5pt). Encrypt the message "do not attack" using the following ciphers. Ignore the space between the words. Decrypt the message to get the original plaintext. (note: please ignore the spaces)

a). Additive cipher with key = 12

Plaintext: d=> 03 Encryption: (3 + 12) mod 26 Ciphertext:15 => P
Plaintext: o => 14 Encryption: (14 + 12) mod 26 Ciphertext: 00 => A
Plaintext: n=> 13 Encryption: (13 + 12) mod 26 Ciphertext: 25 => Z
Plaintext: o => 14 Encryption: (14 + 12) mod 26 Ciphertext: 00 => A
Plaintext: t => 19 Encryption: (19 + 12) mod 26 Ciphertext: 5 => F
Plaintext: a => 00 Encryption: (0 + 12) mod 26 Ciphertext:12 => M
Plaintext: t => 19 Encryption: (19 + 12) mod 26 Ciphertext: 5 => F
Plaintext: t => 19 Encryption: (19 + 12) mod 26 Ciphertext: 5 =>F
Plaintext: a => 00 Encryption: (0 + 12) mod 26 Ciphertext: 12 => M
Plaintext: c => 02 Encryption: (2+ 12) mod 26 Ciphertext: 14 => O
Plaintext: k => 10 Encryption: (10 + 12) mod 26 Ciphertext: 22 => W

The encrypted message is: PAZAFMFFMOW

b). multiplicative cipher with key = ~~11~~ 15

Plaintext: d=> 03 Encryption: (3 * 15) mod 26 Ciphertext:19 => T
Plaintext: o => 14 Encryption: (14 * 15) mod 26 Ciphertext: 2 => C
Plaintext: n=> 13 Encryption: (13 *15) mod 26 Ciphertext: 13 => N
Plaintext: o => 14 Encryption: (14 * 15) mod 26 Ciphertext: 2 => C
Plaintext: t => 19 Encryption: (19 * 15) mod 26 Ciphertext: 25 => Z
Plaintext: a => 00 Encryption: (0 *15) mod 26 Ciphertext:0 => A
Plaintext: t => 19 Encryption: (19 * 15) mod 26 Ciphertext: 25 => Z
Plaintext: t => 19 Encryption: (19 * 15) mod 26 Ciphertext: 25 =>Z
Plaintext: a => 00 Encryption: (0 * 15) mod 26 Ciphertext: 0 => A
Plaintext: c => 02 Encryption: (2*15) mod 26 Ciphertext: 4 => E
Plaintext: k => 10 Encryption: (10* 15) mod 26 Ciphertext: 20 => U

Ciphertext: T C N C Z A Z Z A E U

To decrypt it, we need to find the multiplicative inverse of 15.

q	r1	r2	r	t1	t2	t
1	26	15	11	0	1	-1
1	15	11	4	1	-1	2
2	11	4	3	-1	2	-5
1	4	3	1	2	-5	7
3	3	1	0	-5	7	-26
	1	0		7	-26	

15^{-1} mod 26 = 7

Ciphertext: T=> 19 Decryption: (19 * 7) mod 26 Plaintext:3 => d
Ciphertext: C => 2 Decryption: (2 * 7) mod 26 Plaintext: 14 => o
Ciphertext: N=> 13 Decryption: (13 *7) mod 26 Plaintext: 13 => n
Ciphertext: C => 14 Decryption: (14 * 7) mod 26 Plaintext: 14 => o
Ciphertext: Z => 25 Decryption: (25 * 7) mod 26 Plaintext: 19 => t
Ciphertext: A => 00 Decryption: (0 *7) mod 26 Plaintext:0 => a
Ciphertext: Z => 25 Decryption: (25 * 7) mod 26 Plaintext: 19 => t
Ciphertext: Z => 25 Decryption: (25 * 7) mod 26 Plaintext: 19 =>t
Ciphertext: A => 00 Decryption: (0 * 7) mod 26 Plaintext: 0 => a
Ciphertext: E => 4 Decryption: (4*7) mod 26 Plaintext: 2 => c
Ciphertext: U=> 20 Decryption: (20* 7) mod 26 Plaintext: 10 => k

c). Affine cipher with key = (15,12)

Plaintext: d=> 03 Encryption: (3 * 15+12) mod 26 Ciphertext:5 => F

Plaintext: o => 14 Encryption: (14 * 15+12) mod 26 Ciphertext: 14 => O
Plaintext: n=> 13 Encryption: (13 *15+12) mod 26 Ciphertext: 25 => Z
Plaintext: o => 14 Encryption: (14 * 15+12) mod 26 Ciphertext: 14 => O
Plaintext: t => 19 Encryption: (19 * 15+12) mod 26 Ciphertext: 11 => L
Plaintext: a => 00 Encryption: (0 *15+12) mod 26 Ciphertext:12 => M
Plaintext: t => 19 Encryption: (19 * 15+12) mod 26 Ciphertext: 11=> L
Plaintext: t => 19 Encryption: (19 * 15+12) mod 26 Ciphertext: 11=>L
Plaintext: a => 00 Encryption: (0 * 15+12) mod 26 Ciphertext: 12 => M
Plaintext: c => 02 Encryption: (2*15+12) mod 26 Ciphertext: 16 => Q
Plaintext: k => 10 Encryption: (10* 15+12) mod 26 Ciphertext: 6 => G

The ciphtertext: F O Z O L M L L M Q G

Decryption:

Ciphertext: F=> 5 Decryption: ((5-12) * 7) mod 26 Plaintext:3 => d
Ciphertext: O => 14 Decryption: ((14-12) * 7) mod 26 Plaintext: 14 => o
Ciphertext: Z=> 25 Decryption: ((13-12) *7) mod 26 Plaintext: 13 => n
Ciphertext: O => 14 Decryption: ((14-12) * 7) mod 26 Plaintext: 14 => o
Ciphertext: L => 11 Decryption: ((25-12) * 7) mod 26 Plaintext: 19 => t
Ciphertext: M => 12 Decryption: ((0-12) *7) mod 26 Plaintext:0 => a
Ciphertext: L => 11 Decryption: ((25-12) * 7) mod 26 Plaintext: 19 => t
Ciphertext: L => 11 Decryption: ((25-12) * 7) mod 26 Plaintext: 19 =>t
Ciphertext: M => 12 Decryption: ((0-12) * 7) mod 26 Plaintext: 0 => a
Ciphertext: Q => 16 Decryption: ((4-12)*7) mod 26 Plaintext: 2 => c
Ciphertext: G=> 6 Decryption: ((20-12)* 7) mod 26 Plaintext: 10 => k

---

5.(1pt). a) Construct a Playfair key matrix with the keyword "university"
b) Use the matrix created in a) to encrypt the message "attackistomorrow"

u	n	i/j	v	e
r	s	t	y	a
b	c	d	f	g
h	k	l	m	o
p	q	w	x	z

Plaintext pairs

at	ta	ck	is	to	mo	rx	ro	wx

Ciphertext

RY	YR	KQ	NT	AL	OH	YP	AH	XZ

---

6. (0.5pt). The encryption key in a transposition cipher is
(5, 12, 3, 7, 9, 6, 4, 14, 1, 13, 10 , 8, 15, 2, 11,16).
Find the decryption key

Add indices:
(5, 12, 3, 7, 9, 6, 4, 14, 1, 13, 10 , 8, 15, 2, 11,16)
1, 2 , 3 , 4, 5, 6, 7, 8, 9 ,10,11, 12,13, 14,15,16

Swap contents and indices:
(1, 2 , 3 , 4, 5, 6, 7, 8, 9 ,10, 11, 12,13, 14,15,16)
5, 12, 3, 7, 9, 6, 4, 14, 1, 13, 10 , 8, 15, 2, 11,16

Sort based on indices:
(9, 14, 3 , 7, 1 6 4 12 5 11 15 2 10 8 13 16)
01, 02, 03, 04, 05, 06, 07, 08, 09 ,10, 11, 12, 13, 14, 15, 16

The decryption key is: (9, 14, 3 , 7, 1 ,6 , 4 , 12 , 5 , 11 , 15, 2, 10, 8, 13, 16)

---

7. (0.5pt) Show that an integer N is congruent modulo 9 to the sum of its decimal digits. For example, 475 ≡ 4+7+5 ≡ 16 ≡ 1+6 ≡ 7 (mod 9).
Any integer N can be written in the following format:
$N = a_p*10^p + a_{p-1}*10^{p-1} + \ldots +a_2*10^2 + a_1*10+a0$
Where $a_0,a_1,\ldots a_p$ are its decimal digits, p is an integer.
So N mod 9 = $(a_p*10^p + a_{p-1}*10^{p-1} + \ldots +a_2*10^2 + a_1*10+a0)$ mod 9
= $[(a_p*10^p \text{ mod } 9) + (a_{p-1}*10^{p-1} \text{ mod } 9) + \ldots + (a0 \text{ mod } 9)]$ mod 9
=$[a_p *(10^p \text{ mod } 9) +a_{p-1} *(10^{p-1} \text{ mod } 9) + \ldots + (a0 \text{ mod } 9)]$ mod 9
=$(a_p + a_{p-1} +\ldots+a0)$ mod p (because 10^p mod 9 = 1)