1 (0.5pt). What integers do the sets Z28 and Z28\* contain?  For each set, list all additive inverse pairs  and multiplicative inverse pairs.

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),(9,25),(11,23),(13,13),(15,15),(27,27)

2 (1pt).   Using extended Euclidean algorithm, show the steps of finding the following multiplicative inverses - a ≡ b-1 mod n

1. 321-1 mod 56709 – There is no inverse because GCD is not 1;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Q | R1 R2 | R | T1 T2 | T |
| 176 | 56709 321 | 213 | 0 3 | -528 |
| 1 | 321 213 | 108 | 3 -528 | 531 |
| 1 | 213 108 | 105 | -528 531 | -1059 |
| 1 | 108 105 | 3 | 531 -1059 | 1590 |
| 35 | 105 3 | 0 | -1059 1590 | -56709 |
|  | 3 0 |  | 1590 -56709 |  |

1. 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 |  |

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

a)24x ≡ 12 (mod 28) ; GCD(24, 28) = 4; 12/4 = 3 (there are 4 solutions)

6x ≡ 3(mod 7) 🡪 x ≡ 3 (6­­­-1) (mod 7)

x0 = (3 X 6-1) mod 7 = (3x6) (mod 7) = 4;

x1 = x0 + 1(28/4) = 11;

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

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

b) 4x  + 5 ≡ 17(mod 10) 🡪 4x ≡ 12 (mod 10); GCD(4,10) = 2. 12/2 = 6. (2 solutions.)

2x ≡ 6 (mod 5) 🡪 x ≡ 6(2-1) (mod 5)

x0 = (6\*3) (mod 5) = 3;

x1 = x0 + 1(10/2) = 8;

c) 5x ≡ 15(mod 25); GCD(25,5) = 5; 15/5 = 3; (5 solutions)

x ≡ 3(mod 5) ;

x0= 3(mod 5) = 3;

x1 = x0 + 1(25/5) = 8;

x2 = x0 + 2(25/5) = 13;

x3 = x0 + 3(25/5) = 18;

x4 = x0 + 4(25/5) = 23;

d) 24x +20 ≡ 29 (mod 69) 🡪 24x ≡ 9 (mod 69) GCD(69, 24) = 3; 9/3 = 3; (3 solutions)

x = 3 (8-1) (mod 23)

x0  = (3 \* 3) (mod 23) = 9;

x1 = 9 + 1(9/3) = 12;

x2 = 9 + 2(3) = 15;

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 ; C = (p + 12) mod26;

“do not attack” = “pazafmffmow” – with no spaces

d = (3 + 12) mod 26 = 15 = p ; o = (14 + 12) mod 26 = 0 = a; n = (13+12) mod 26=25=z;

t =(19+12)mod26=5=f; a=(0+12)mod26=12=m; c=(2 + 12)mod26 =14 =o;

k =(10+12)mod26 = 22 = w;

decrypt = P = (C-k) mod26; pazafmffmow = “do not attack”

p = (15 – 12)mod26 =3=d; a= (0-12)mod26 =14=o; z=(25-12)mod26 = 13=n;

f =(5-12) mod26 =19= t; m=(12-12)mod26=0= a; o=(14-12)mod26 = 2 = c;

w = (22-12)mod26 = 10= k

b). multiplicative cipher with key = ~~11~~ 15 C= (p\*k) mod 26

“do not attack” = tc ncz azzaeu

d=(3\*15) mod 26 = 19 = t ; o = (14\*15) mod 26 = 2 = c ; n=(13\*15) mod 26 = 13 = n;

t=(19\*15)mod26 = 25 = z; a = (0\*15)mod26 = 0 =a; c=(2\*15)mod26 = 4 = e;

k = (10\*15)mod26 = 20 = u;

decrypt = P = (C \* k­-1)mod26; 15-1 mod 26 = 7 ; tc ncz azzaeu =

t = (7\*19)mod 26 = 3 = d; c =(7\*2)mod26 = 14 = o; n = (13 \* 7) mod26= 13 = n;

z = (25\*7) mod26 = 19 = t ; a= (7\*0)mod26 = 0=a; e = (4\*7) mod26 = 2 = c;

u = (20\*7)mod26 = 10 = k;

c). Affine cipher with key = (15,12) ; T = (p \* k1); C = (T + k2)

“do not attack” = fo zol mllmqg

d = ((3 \* 15) + 12) mod 26 = 5 = f; o = ((14 \* 15) + 12) mod26 = 14 = o;

n = ((13 \* 15) +12) mod26 = 25 = z; t = ((19\*15) + 12) mod26 = 11 = l;

a = ((0\*15)+12) mod 26 = 12 = m; c = ((2\*15)+12) mod 26 = 16 = q;

k = ((10\*15)+12)mod26 = 6 = g;

decrypt = P = (T \* k1-1) ; T = (C – k2); k1-1 = 7;

“fo zol mllmqg” = do not attack

f = ((5 – 12) \* 7) mod 26 = 3 = d; o =((14-12)\*7)mod26 = 14 = o;

z = ((25-12) \*7) mod 26 = 13 = n; l =((11-12)\*7)mod 26 = 19 = t;

m = ((12-12)\*7) mod26 = 0 = a; q=((16-12)\*7) mod 26 = 2 = c;

g = ((6-12)\*7) mod 26 = 10 = k;

5.(1pt). a) Construct a Playfair key matrix with the keyword  "university"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

     b) Use the matrix created in a) to encrypt the message "attackistomorrow"

at ta ck is to mo rx ro wq

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

(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 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).

576 ≡ 5 + 6 + 7 = 18 ≡ 0 mod 9

323 ≡ 3 + 2 + 3 ≡ 8 ≡ 8 mod 9;

25 ≡ 2 + 5 ≡ 7 mod 9

12345 ≡ 1 + 2 + 3 +4 + 5≡ 15 ≡ 6 mod 9