## Homework 1

1.What integers do the sets Z38 and Z38\* contain? List all additive inverse pairs  and multiplicative inverse pairs in the two sets.

2. Using extended Euclidean algorithm, show the steps of finding the following multiplicative inverses

a)     323-1 mod 80979.

b)     159-1 mod 56478

3. For the group G = <Z32\*, x>

a. Find the order of the group

b. Find the order of each element in the group

4. Using the irreducible polynomial f(x) = x5+x4+x3+x+1   to

a) generate the elements of the field GF(25)

b) **based on the results of a)**, calculate the followings in GF(25)

   b.1) (x2 + x+ 1)-1

   b.2) (x3- x + 1) X (x3 + x2 + 1)

   b.3) (x4- x + 1) / (x3 + x + 1)

5. Find the results of following, using Fermat's little theorem or Euler's theorem.

a)  267039962 mod 59

b) 37-1 mod 416

c) 79-1 mod 398

d) 59 -1 mod 676

e) 38433999802  mod 448