COMP90043 Cryptography and Security
Semester 2, 2021, Workshop Week 11

Tasks:

1. What are differences between $\mathbf{GF}(8)$ and $\mathbf{Z}_8$?

2. Describe the conditions under which $\mathbf{GF}(m)$ and $\mathbf{Z}_m$ are identical.

3. For any finite field of size p^k, p is a prime number, k is an integer ≥ 1, $a \in \mathbf{GF}(p^k)$ and $a \neq 0$, we have
$$a^{p^k-1} = 1.$$
Use this result to derive a function for determining inverse of an element in $\mathbf{GF}(p^k)$.

4. Use the irreducible polynomial $x^4 + x + 1$ to create a table for the finite field $GF(16)$.

i	Elements:x^i	As Polynomials	As Vectors	Multiplicative Order
$-\infty$	0	0	$[0,0,0,0]$	
0	1	1	$[0,0,0,1]$	
1	x	x	$[0,0,1,0]$	
2	x^2	x^2	$[0,1,0,0]$	
3	x^3	x^3	$[1,0,0,0]$	
4	x^4			
5	x^5			
6	x^6			
7	x^7			
8	x^8			
9	x^9			
10	x^{10}			
11	x^{11}			
12	x^{12}			
13	x^{13}			
14	x^{14}			
15	x^{15}			

   (a) Complete the missing entries in the table.

   (b) Determine multiplicative order of elements.

   (c) What's the multiplicative inverse of $x^3 + x^2$?

5. Derive the verification equations of the ElGamal signature using the defining equations of signing.

6. Discuss ElGamal digital signature scheme with an example. Say, for $q = 19$ and $\alpha = 13$, $m = 7$, calculate the signature and verify it.