COMP90043: Cryptography and security: Week 10, Part B: ElGamal Signatures

(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 filed of size p^k, p, a prime number and k, an integer than or equal to 1, show that

$$a^{p^m-1} = 1,$$

where $a \in \mathbf{GF}(p^k - 1)$ and $a \neq 0$.

(4) Use the above result to derive a function for determining inverse of an element in $\mathbf{GF}(p^k)$.

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

Note: Please read slides 4, 5 and 9 before attempting this question.

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

(7) Show that verification equations of Schnorr's signature scheme follows from the signing equation.

(8) How do you determine primes p and q as required for the Schnorr's signature scheme? Suggest a method. Given an example in small primes.