COMP90043: Cryptography and security: Week 7: Polynomial Rings and Finite Field

(1) Consider a finite filed $\mathbf{F}_5$, the field of 5 elements. Given an example for each of the following:
   (a) A polynomial of degree 3.
   (b) A monic polynomial of degree 3
   (c) An irreducible polynomial of degree 2.

(2) Consider a finite filed $\mathbf{F}_3$, the field of 3 elements. Answer the following:
   (a) $(1 + 2\ x + x^3) * (1 + x^2 + 2\ x^3) =$ ________________.
   (b) $x^5\ mod\ (1 + 2\ x + x^3) =$ ________________.
   (c) An irreducible polynomial of degree 2= ________________-.
   (d) $GCD((1 + 2x + x^3), (1 + 2x))=$ ________________.
   (e) Is the polynomial $2 + 2 * x^2$ is an irreducible polynomial?

(3) Use the irreducible polynomial $1 + x^2 + x^3$ in the the finite field $GF(8)$ table below:

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0, 0, 0]$
0	1	1	$[1, 0, 0]$
1	x	x	$[0, 1, 0]$
2	x^2	x^2	$[0, 0, 1]$
3	x^3	$1 + x^2$	$[1, 0, 1]$
4	x^4		
5	x^5		
6	x^6		
7	x^7		

Table 1. Elements of $GF(2^3)$ as powers of x

   (a) Complete the missing entries in the table.
   (b) What is the multiplicative order of x?
   (c) What is the multiplicative inverse of x^3?
   (d) Compute $x + x^2 + x^4$.
   (e) Compute $x^3 + x^6 + x^5$;

(4) Consider the finite field $GF(9)$ as discussed in class last week:

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0,0]$
0	1	1	$[1,0]$
1	x	x	$[0,1]$
2	x^2		
3	x^3		
4	x^4		
5	x^5		
6	x^6		
7	x^7		
8	x^8		

TABLE 2. Elements of $GF(3^2)$ as powers of x

(a) Complete the missing entries by using the polynomial $2+x+x^2$ as the irreducible polynomial for generating powers of x in the table.

(b) What is the multiplicative order of x?

(c) What is the multiplicative inverse of x^2?

(d) Compute $x + x^3$.

(e) Compute $x^2 + x^6$;

(5) Homework: Generate tables for $GF(2^4)$ and $GF(2^5)$ using primitive polynomials of degree 4 and 5 respectively.

(6) Homework: Implement extended GCD algorithms for polynomials over finite field.