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: $1 + x + 3 * x^3 + 4x^3$.
   (b) A monic polynomial of degree 3: $1 + x + 3 * x^3 + x^3$.
   (c) An irreducible polynomial of degree 2. $1 + 2x^2$;

(2) Consider a finite filed $\mathbf{F}_3$, the field of 3 elements. Answer the following:
   (a) $(1 + 2\ x + x^3) * (1 + x^2 + 2\ x^3) = 2 * x^6 + x^5 + x^4 + 2 * x^3 + x^2 + 2 * x + 1$.
   (b) $x^5\ mod\ (1 + 2\ x + x^3) = 2 * x^2 + x + 2$.
   (c) An irreducible polynomial of degree 2= $x^2 + 1; x^2 + 2 * x + 2; x^2 + x + 2$.
   (d) $GCD((1 + 2x + x^3), (1 + 2x))$= 1.
   (e) Is the polynomial $2 + 2 * x^2$ is an irreducible polynomial? Yes

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

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	$1 + x + x^2$	$[1, 1, 1]$
5	x^5	$1 + x$	$[1, 1, 0]$
6	x^6	$x + x^2$	$[0, 1, 1]$
7	x^7	1	$[1, 0, 0]$

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

   (a) Complete the missing entries in the table.
   (b) What is tye multiplicative order of x? 7.
   (c) What is the multiplicative inverse of x^2? x^5

(d) Compute $x + x^2 + x^4 : 1$

(e) Compute $x^3 + x^6 + x^5 : 0$

(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	$1 + 2 * x$	$[1, 2]$
3	x^3	$2 + 2x$	$[2, 2]$
4	x^4	2	$[2, 0]$
5	x^5	$2x$	$[0, 2]$
6	x^6	$2 + x$	$[2, 1]$
7	x^7	$1 + x$	$[1, 1]$
8	x^8	1	$[1, 0]$

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? 8

(c) What is the multiplicative inverse of x^2? x^6

(d) Compute $x + x^3$. 2

(e) Compute $x^2 + x^6$ 0;