Homework 12

Question 1

(a) Complete the following multiplication table.

	0	1	x	x^2	$1+x$	$1+x^2$	$x+x^2$	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	x			$1+x^2$	$x+x^2$	$1+x+x^2$
x	0	x	x^2		$x+x^2$	1		$1+x^2$
x^2	0			$x+x^2$	$1+x+x^2$	x	$1+x^2$	1
$1+x$	0		$x+x^2$	$1+x+x^2$	$1+x^2$		1	x
$1+x^2$	0	$1+x^2$	1	x		$1+x+x^2$	$1+x$	
$x+x^2$	0	$x+x^2$		$1+x^2$	1	$1+x$	x	
$1+x+x^2$	0	$1+x+x^2$	$1+x^2$	1	x			$1+x$

Table 2.5: Multiplication table for the field $\mathbb{F}_2[x]/(x^3+x+1)$

(b) Draw the multiplication table for the field $\mathbb{F}_2[x]/(x^3+x^2+1)$.

(c) Show that $\mathbb{F}_2[x]/(x^3+x+1)$ is isomorphic to $\mathbb{F}_2[x]/(x^3+x^2+1)$.

Question 2

(a) Show that x^2+1 irreducible in $\mathbb{F}_3[x]$. (Show that no polynomial of degree 1 in $\mathbb{F}_3[x]$ that divides x^2+1.)

(b) Show that x^2+1 is not irreducible in $\mathbb{F}_5[x]$. (Find a polynomial of degree 1 in $\mathbb{F}_5[x]$ that divides x^2+1)

(c) For what values of p does x^2+1 is irreducible in $\mathbb{F}_p[x]$?

Justify your answers.

Question 3

Let $F = \mathbb{F}_3[x]/(x^2+1)$. F is a field because x^2+1 is irreducible in $\mathbb{F}_3[x]$ (see Question 1a).

(a) How many elements are there in F?

(b) Does x generate $F \setminus \{0\}$? Justify your answer.

(c) Does $x+1$ generate $F \setminus \{0\}$? Justify your answer.

Question 4

(a) Consider the (3, 6)-Shamir threshold scheme to share a secret in $\mathbb{F}_{19}$.

Suppose that participants P_2, P_3, P_6 pool their shares:

$(2, 8)$, $(3, 18)$, $(6, 11)$

Compute the secret.

(b) Show that if only P_2 and P_3 pool their shares: $(2, 8)$, $(3, 18)$, they have no information on the secret. In other words, just with the knowledge of $(2, 8)$, $(3, 18)$, the secret key can be any value in $\mathbb{F}_{19}$.

(Show that there exists a polynomial of degree 2 that fits $(2, 8)$, $(3, 18)$, $(0, s)$ for all values of $s \in \mathbb{F}_{19}$)

Question 5

In Shamir secret sharing scheme, the dealer who distributes the shares to participants is assumed to be honest.

A malicious dealer could give invalid shares to some people, so that any t people involving at least one of them would compute the wrong secret.

To prevent this, one strategy is to ask the dealer to publish $g^{a_0}, g^{a_1}, \dots, g^{a_{t-1}}$ where $a_0, a_1, \dots, a_{t-1}$ are the coefficients of the secret polynomial $f(x)$, and g is an element of large prime order.

(a) Show how each participant P_i can verify that the share $(i, f(i))$ he/she received is valid using values $g_i = g^{a_i}, 0 \le i \le t-1$, that the dealer published.

Note that $a_0, a_1, \dots, a_{t-1}$ are private/unknown to public.

(b) Is such verification scheme secure? In other words, could anyone find out the secret value using the publish values $g^{a_0}, g^{a_1}, \dots, g^{a_{t-1}}$?