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) Prove that x^3+x^2+1 is irreducible over $\mathbb{F}_2$.

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

(d) 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 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	x^2	$1+x$	$1+x^2$	$x+x^2$	$1+x+x^2$
x	0	x	x^2	$x+1$	$x+x^2$	1	x^2+x+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) Prove that x^3+x^2+1 is irreducible over $\mathbb{F}_2$.

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

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

(a) $x \cdot x^2 = x^3 \mod(x^3+x+1)$ $\qquad x^3 = -x-1$
$= x+1$ $\qquad = x+1$

$x \cdot (x+x^2) = x^2+x^3 \mod (x^3+x+1)$
$= x^2+x+1$

(b) Idea: Show that there is no polynomial of degree < 3 that divides $f(x) = x^3+x^2+1$.

If $f(x)$ is reducible over $\mathbb{F}_2$, then $f(x) = g(x)h(x)$ where $1 \leq dg(g), dg(h) < 3$.

Idea: If $f(x)$ is reducible then, there exist $a \in \mathbb{F}_2$ s.t $x-a$ divides $f(x)$. If $x-a$ divides $f(x)$ then a is a root of $f(x)$.

$f(0) = 0^3+0^2+1 = 1$, 0 is not a root

$f(1) = 1+1+1 = 1$, 1 is not a root.

Since $f(x)$ does not have a root in $\mathbb{F}_2$, $f(x)$ is irreducible over $\mathbb{F}_2$.

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	x^2	$1+x$	$1+x^2$	$x+x^2$	$1+x+x^2$
x	0	x	x^2	$x+1$	$x+x^2$	1	x^2+x+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) Prove that x^3+x^2+1 is irreducible over $\mathbb{F}_2$.

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

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

(c) $x^3+x^2+1 = 0$

$x^3 = -x^2-1 = x^2+1$ in $\mathbb{F}_2[x]$

(d) $\mathbb{F}_2[x]/(x^3+x+1)$ $2^3 = 8$ elements

$\mathbb{F}_2[x]/(x^3+x^2+1)$ $2^3 = 8$ elements

(Recall $\mathbb{F}_2[x]/(x^3+x+1) \setminus \{0\}$ is a cyclic group with 7 elements. So, there are $\varphi(7) = 6$ generators)

In $\mathbb{F}_2[x]/(x^3+x+1)$, x is a generator of the non-zero element.
x is such that $x^3 = x+1$

In $\mathbb{F}_2[x]/(x^3+x^2+1)$, x is a generator of the non-zero element.
x is such that $x^3 = x^2+1$

Let α such that $\alpha^3 = \alpha+1$.
Let β such that $\beta^3 = \beta^2+1$
Write α in terms of β. $[\alpha = a_0 + a_1\beta + a_2\beta^2]$

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.

(a) $f(x) = x^2+1$. If $f(x)$ has proper divisor, then it is divisible by $(x-a)$, $a \in \mathbb{F}_3$.

$f(0) = 1$, $f(1) = 2$, $f(2) = 2$

So, $f(x)$ has no root in $\mathbb{F}_3[x]$, so, $f(x)$ is irreducible over $\mathbb{F}_3$

(b) $f(x) = x^2+1$. $f(0) = 1$, $f(1) = 2$, $f(2) = 5 = 0$

$f(x) = (x-2) g(x)$

(c) x^2+1 is irreducible over $\mathbb{F}_p$ when $p \equiv 3 \bmod 4$.

x^2+1 is reducible iff x^2+1 has a root in $\mathbb{F}_p$.

iff $x^2 = -1 \bmod p$

iff -1 is QR mod p

iff $p \equiv 1 \bmod 4$

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 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.

(a) $3^2 = 9$

(b) In F, $x^2+1=0 \Rightarrow x^2 = -1 \equiv 2 \bmod 3$

$x, \ x^2 = 2, \ 2x, \ 2x^2 = 1$

So, $\langle x \rangle = \{x^i \text{ in } F\} = \{x, 1, 2, 2x\}$

(c) $x+1$, $(x+1)^2 = x^2+2x+1 = 2x$, $(2x)(x+1) = 2x^2+2x = 2x+1$, $(2x+1)(x+1) = 2x^2+x+2x+1 = 4+3x+1 = 5+3x = 2$

$\langle x+1 \rangle = \{(x+1)^i \text{ in } F\} = \{ \ ? \qquad \}$

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 $s \in \mathbb{F}_{19}$)

(a) Just use Lagrange Interpolation to compute $f(x)$.

$f(x) = a_0 + a_1 x + a_2 x^2$

a_0 is the secret.

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

Find $f(0)$.

(b) Let $f(x) = a_0 + a_1 x + a_2 x^2 \in \mathbb{F}_{19}[x]$.

Find $f(x)$ such that $f(2) = 8$, $f(3) = 18$, $f(0) = S$

Question

Consider the following (6, 6) secret-sharing scheme.
The secret key is a bit string of 12 bits.

Distribute the shares to each participant:

participant 1 gets the first 2 bits $b_0 b_1$
participant 2 gets the subsequent 2 bits $b_2 b_3$
⋮
participant 6 gets the last 2 bits. $b_{10} b_{11}$

(a) How do all participants compute the secret?

concatenate all the shares: $b_0 b_1 b_2 \ldots b_{11}$

(b) Can less than 6 participants compute the secret?

If first 5 participants pool their shares together, then get $b_0 b_1 \ldots b_9 \underline{?}\,\underline{?}$

which implies that secret key can only be one of the four possibilities
$b_0 b_1 \ldots b_9 00$, $b_0 b_1 \ldots b_9 01$, ...

Out of the 2^{12} possibilities, we rule out $2^{12} - 4$ of them.

This is not secure!

Question 5 Verifiable Secret Sharing Scheme

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 $g^{a_0}, g^{a_1}, \ldots, g^{a_{t-1}}$ where $a_0, a_1, \ldots, a_{t-1}$ 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 $a_0, a_1, \ldots, a_{t-1}$ 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 $g^{a_0}, g^{a_1}, \ldots, g^{a_{t-1}}$?

Hint: If you solve DLP, can you get the secret?

(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 $g^{a_0}, g^{a_1}, \dots, g^{a_{t-1}}$?

Hint: If you solve DLP, can you get the secret?

(a) $i, f(i), g^{a_0}, g^{a_1}, \dots, g^{a_{t-1}}, g$

$$f(i) = a_0 + a_1 i + a_2 i^2 + \dots + a_{t-1} i^{t-1}$$

$$g^{f(i)} = g^{a_0 + a_1 i + a_2 i^2 + \dots + a_{t-1} i^{t-1}}, \quad g_i = g^{a_i}$$

$$= g_0 \cdot g_1^{i} \cdot g_2^{i^2} \cdot \dots$$

Compute $g^{f(i)}$ as X

Compute $g_0 g_1^{i} g_2^{i^2} \dots g_t^{i^{t-1}}$ as Y.

Accept $f(i)$ iff X is equal to Y.