Name: Rajat Rajesh shetty
CWID: 10477484.

Assignment-10

Exercise 10.1

consider $f(x) = x^2+2x+2 \in \mathbb{Z}_3(x)$.

(a) S.T $f(x)$ is irreducible.

(b) Let $E = \mathbb{Z}_3[x]/\langle f(x) \rangle$ what is $\chi(E)$?

(a) $\mathbb{Z}_3 : \{0, 1, 2\}$.

$f(x) = x^2+2x+2$.

$f(0) = 0^2+0+2 \equiv_3 2 \neq 0$.

$f(1) = 1+2+2 = 5 \equiv_3 2 \neq 0$.

$f(2) = 2^2+2\cdot 2+2 = 10 \equiv_3 1 \neq 0$,

hence $f(x) = x^2+2x+2$ is irreducible in $\mathbb{Z}_3$.

(b). $\chi(E) = 3$,

because.

$3 \cdot f(x) \equiv_3 0$.

$3(x^2+2x+2) = 3x^2+6x+6 \equiv_3 0$

$= 27+18+6 = 51 \equiv_3 0$.

so, $\chi(E) = 3$

Exercise 10.2 consider the following elements in $E = \mathbb{Z}_3[x]/(x^2+2x+2)$.

$a = 2x+1,\ b = x+2,\ c = x.$

(a) compute the unique representives for $a \cdot b$ & $a+b$. Dont use any software.

$\Rightarrow$ $a \cdot b = (2x+1)(x+2) = 2x^2+4x+x+2 = 2x^2+5x+2 = 2x^2+2x+2$
$= 2(x^2+x+1)$

$\therefore a \cdot b = 2(x^2+x+1) = 2((x+1)+(x+1)) = 2(2x+2) = 4x+4$
$\Rightarrow x+1$ //

Now, $a+b = (2x+1)+(x+2) = 3x+3 = 0$ //

(b) Find c^{-1} in E. Dont use any software.

$\Rightarrow$ Let $ax+b$, $a, b \in \mathbb{Z}_3$ is c^{-1} where $c = x$.

$\therefore\ c(ax+b) = 1$
$x(ax+b) = 1$
$ax^2+bx = 1$
$a(x+1)+bx = 1$
$(a+b)x+a = 1$
$\Rightarrow a+b = 0$ & $a = 1$ $\Rightarrow a = 1;\ b = -1 = 2$ //

So, the $\underset{c^{-1}}{x^{-1}}$ is $(x+2)$ //

Exercise 10.2.

c) Compute all distinct power of a in E. You are allowed to use wolfram Alpha for this question.

PolynomialMod [$(2x+1)^{15}$, $\{3, x^2+2x+2\}$].

$\Rightarrow$ $a = 2x+1$. ; polyMod : x^2+2x+2.

$(2x+1)^2 = (2x+1)(2x+1) = x^2+x+1 \equiv_{f(x)} 2x+2$.

$(2x+1)^3 = (2x+2)(2x+1) = x^2+2 \equiv_{f(x)} x$.

$(2x+1)^4 = (2x+2)\cdot x = 2x^2+x \equiv_{f(x)} 2$.

$(2x+1)^5 = (2.)(2x+1) = x+2 \equiv_{f(x)} (x+2)$

$(2x+1)^6 = (x+2).(2x+1) = 2x^2+2x+2 \equiv_{f(x)} x+1$.

$(2x+1)^7 = (x+1)(2x+1) = 2x^2+1 \equiv_{f(x)} 2x$.

$(2x+1)^8 = (2x).(2x+1) = x^2+2x \equiv_{f(x)} 1$.

$(2x+1)^9 = 2x+1 = a$;

Therefore, in $\mathbb{Z}_3[x] / x^2+2x+2$, we have the following.

$\log_{2x+1}(1) = 0$, $\log_{(2x+1)}(2x+1) = 1$, $\log_{2x+1}(2x+2) = 2$.

$\log_{2x+1}(x) = 3$, $\log_{2x+1}(2) = 4$, $\log_{2x+1}(x+2) = 5$

$\log_{2x+1}(x+1) = 6$, $\log_{(2x+1)}(2x) = 7$, $\log_{2x+1}(1) = 8$

(d) Find $|a|$ in E^*. is a primitive in E?

$|a| = p^n - 1$ in E^*

Hence, $|a| = 3^2 - 1 = 9 - 1 = 8$

$PPF(p^n-1) = 9-1 = 8 = 2^2.2$.

Hence $a = (2x+1)$ is a primitive root if and only if

$2x+1^{\frac{p^n-1}{p_i}} \neq 1 \Rightarrow (2x+1)^{8/4} = (2x+1)^2$.

$\Rightarrow (2x+1)^{8/2} = (2x+1)^4$.

From 10.2 (c), $(2x+1)^2 = x^2+x+1$ & $(2x+1)^4 = 2x^2+x$.

now lets check if $(2x+1)$ is a primitive root.

* $x^2+x+1 \neq 1 \mod x^2+2x+2 \Rightarrow$ true.

$$\begin{array}{r|l} & 1 \\ \hline x^2+2x+2 & x^2+x+1 \\ & -x^2+2x+2 \\ \hline & 2x+2 \end{array}$$

* $2x^2+x \neq 1 \mod x^2+2x+2 \Rightarrow$ true

$$\begin{array}{r|l} & 2 \\ \hline x^2+2x+2 & 2x^2+x \\ & -2x^2+x+1 \\ \hline & -1 \Rightarrow 2 \text{ in } Z_3. \end{array}$$

Hence, $2x+1$ is a primitive root in E.

(e)

For $\alpha, \beta \in E$ the logarithm $\log_\alpha(\beta)$ to the base α is s if $\beta = \alpha^s$

use the powers from (c) to compute $\log_{(2x+1)}(2x+2)$ & $\log_{2x+1}(x+1)$

$\Rightarrow$ using the solution of 10.2. (c),

we know that

$$\log_{2x+1}(2x+2) = 2.$$

& $$\log_{2x+1}(x+1) = 6$$

(f). Alice & Bob run the diffie hellman key exchange protocol in the field E using the base element $g = 2x+1$ if the Alice public key is $A = x$ & Bob's public key is $B = x+1$, then what is their shared key? in other words, solve the instance $CDH(2x+1; x, x+1)$ of the computational Diffie-Hellman problem.

$\Rightarrow$ given

$g = 2x+1$ $A = x$ $B = x+1$.

from 10.2 (c) & given value of A & B,

we can conclude that,

$a = 3$, $b = 6$.

Hence, computing the shared key (proposed by Alice):

$K = B^a \% p.$

$= (x+1)^3 \bmod x^2+2x+2$

$= 2x+2 \bmod x^2+2x+2$

$\boxed{K = 2x+2.}$

* computing the shared key (proposed by bob).

$K = A^b \% p.$

$= x^6 \bmod x^2+2x+2.$

$\boxed{K = 2x+2}$

now, its relatively easy to check that,

$B^a \% p = g^{ab} \% p = A^b \% p.$

so $K = g^{ab} \% p.$

$= (2x+1)^{18} \bmod x^2+2x+2.$

$\Rightarrow (2x+1)^8 + (2x+1)^{10} \bmod x^2+2x+2.$

$= 1 + (2x+2) \bmod x^2+2x+2.$

$= 2x+2 \bmod x^2+2x+2.$

$\boxed{K = 2x+2.}$ shared secret.

Exercise 10.3

Consider a homogenous system of linear. equations with coefficient $\alpha_{ij} \in F$

$$\begin{cases} \alpha_{11}x_1 + \cdots + \alpha_{1t}x_t = 0 \\ \cdots \\ a_{k1}x_1 + \cdots + \alpha_{kt}x_t = 0 \end{cases}$$

S.T the set of solⁿ s; ie, the set

$\{(x_1, \ldots, x_t) \in F^t \mid (x_1 \ldots x_t)$ satisfies the system$\}$.

is a subspace of F^t.

$\Rightarrow$ to show that solⁿ set

$\{(x_1, x_2, \ldots x_t) \in F^t : (x_1, x_2 \ldots x_t))$ satisfies the given system$\}$ is subspace of F^t.

Let $(x_1, x_2, \ldots x_t)$, $(y_1, y_2 \ldots y_t)$ are in the solⁿ set &

$c \in R$.

$a_{11}x_1 + \cdots + a_{1t}x_t = 0$.

$\cdots$

$a_{k1}x_1 + \cdots a_{kt}x_t = 0 \rightarrow (1)$

& $a_{11}y_1 + \cdots + a_{1t}y_t = 0$

$\cdots$

$a_{k1}y_1 + \cdots + a_{kt}y_t = 0 - (2)$

$(1) + c\cdot(2) = a_{11}(x_1 + cy_1) + \cdots + a_{1t}(x_t + cy_t) = 0$

$\cdots$

$\Rightarrow$

$a_{k1}(x_1 + cy_1) + \cdots + a_{kt}(x_t + cy_t) = 0$

$(x_1 + cy_1, \cdots x_t + cy_t) \in$ solⁿ set.

$(x_1, x_2, \ldots x_t) + c(y_1, y_2, \cdots y_t) \in$ the solⁿ set

thus, the solⁿ set of the given system is subspace of F^t.

Exercise 10.4

Consider a case of the blankley secret-sharing (2,3) - threshold scheme in which the dealer uses the field Z_{17} & distributes the following shares?

(#1) $2x_1 + 7x_2 = 7$ — (1)
(#2) $3x_1 + 4x_2 = 8$ — (2)
(#3) $-x_1 + 9x_2 = 0$ — (3)

$z = ax + by + c \mod p$

Let consider

$a_1x + b_1y - z = -c_1 \mod p$
$a_2x + b_2y - z = -c_2 \mod p$
$a_3x + b_3y - z = -c_3 \mod p$

$$\Rightarrow \begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \mod(p).$$ general eq^n:

$$\Rightarrow \begin{pmatrix} 2 & 7 & -1 \\ 3 & 4 & -1 \\ -1 & 9 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \\ 0 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 2 & 7 & -1 \\ 3 & 4 & -1 \\ -1 & 9 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 7 \\ 8 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 8 & 7 & 2 \\ 3 & 2 & 12 \\ 2 & 11 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \\ 0 \end{pmatrix} \bmod$$

$\therefore x_0 = 10 \quad y_0 = 3 \quad z_0 = 0$ The secret ~~key~~ is (10, 3)

$x_0 \Downarrow x_1 \qquad y_0 \Downarrow x_2$

$\Rightarrow$ another method,

(1) + (3) × 2

$$\begin{aligned} 2x_1 + 7x_2 &= 7 \\ -2x_1 + 18x_2 &= 0 \\ \hline 25x_2 &= 7 \end{aligned}$$

$x_2 = \frac{7}{25}$
$\Rightarrow 7 \cdot 25^{-1}$
$\Rightarrow 7 \cdot 15 \Rightarrow 105 \bmod 17 \Rightarrow 3$

$2x_1 + 7 \cdot x_2 = 7$
$2x_1 + 7 \cdot 3 = 7$
$2x_1 + 21 = 7$
$2x_1 = -14$
$x_1 = -7$ in Z_{17} $x_1 \Rightarrow 10$

The secret ~~key~~ is (10, 3)

Exercise 10.5

Unfortunately, one (exactly one!) dishonest participant provided a fake (modified) share. Identify the dishonest participant.

⇒ Given

#1 (12,2),

#2 (3,14),

#3 (9,11),

#4 (7,12).

Lets consider #1 & #2. $\overset{x_1\ y_1}{(12,2)}\ \overset{x_2\ y_2}{(3,14)}$

$$L(x) = y_1\left(\frac{x-x_2}{x_1-x_2}\right) + y_2\left(\frac{x-x_1}{x_2-x_1}\right)$$

$$= 2\frac{(x-3)}{9} + 14\frac{(x-12)}{-9}$$

$$= 2\cdot 9^{-1}(x-3) - 14\cdot 9^{-1}(x-12)$$

$$= 2\cdot 2(x-3) - 14\cdot 2(x-12)$$

$$\Rightarrow 4(x-3) - 28(x-12)$$

$$\Rightarrow 4x-12-28x+336$$

$$\Rightarrow 10x+1 \quad \text{in } \mathbb{Z}_{17}$$

#1 & #3 ⇒ $\overset{x_1\ y_1}{(12,2)}, \overset{x_2\ y_2}{(9,11)}$

$$L(x) = y_1\left(\frac{x-x_2}{x_1-x_2}\right) + y_2\left(\frac{x-x_1}{x_2-x_1}\right)$$

$$= 2\left(\frac{x-9}{12-9}\right) + 11\left(\frac{x-12}{9-12}\right)$$

$$\Rightarrow 2\cdot 3^{-1}(x-9) - 11\cdot 6(x-12)$$

$$\Rightarrow 2\cdot 6(x-9) - 66(x-12)$$

$$\Rightarrow 12\cdot(x-9) - 66x + 792$$

$$= 12x - 108 - 66x + 792.$$

$$\Rightarrow 14x+4$$

#1 & #4. $\overset{x_1\ y_1}{(12, 2)}$ & $\overset{x_2\ y_2}{(7, 12)}$

$$L(x) = y_1\left(\frac{x-x_2}{x_1-x_2}\right) + y_2\left(\frac{x-x_1}{x_2-x_1}\right)$$

$$\Rightarrow 2\left(\frac{x-7}{12-7}\right) + 12\left(\frac{x-12}{7-12}\right)$$

$$\Rightarrow 2\left(\frac{x-7}{5}\right) + 12\left(\frac{x-12}{-5}\right)$$

$$\Rightarrow 2 \cdot 5^{-1}(x-7) - 12 \cdot 5^{-1}(x-12)$$

$$\Rightarrow 2 \cdot 7 \cdot (x-7) - 12 \cdot 7 (x-12)$$

$$\Rightarrow 14(x-7) - 84(x-12)$$

$$\Rightarrow 14x - 98 - 84x + 1008$$

$$\Rightarrow -70x + 910 \Rightarrow 15x + 9 \,//$$

#2 & #3 $\overset{x_1\ y_1}{(3, 14)}$ & $\overset{x_2\ y_2}{(9, 11)}$

$$L(x) = y_1\left(\frac{x-x_2}{x_1-x_2}\right) + y_2\left(\frac{x-x_1}{x_2-x_1}\right)$$

$$\Rightarrow 14\left(\frac{x-9}{3-9}\right) + 11\left(\frac{x-3}{9-3}\right)$$

$6^{-1} = 3$.

$$\Rightarrow 14\left(\frac{x-9}{-6}\right) + 11\left(\frac{x-3}{6}\right)$$

$$\Rightarrow -14 \cdot 6^{-1}(x-9) + 11 \cdot 6^{-1}(x-3) \Rightarrow -42(x-9) + 33(x-3)$$

$$\Rightarrow \underline{\underline{8x+7}}$$

#2 & #4 $\overset{x_1\ y_1}{(3, 14)}$ $\overset{x_2\ y_2}{(7, 12)}$

$$L(x) = y_1\left(\frac{x-x_2}{x_1-x_2}\right) + y_2\left(\frac{x-x_1}{x_2-x_1}\right)$$

$$\Rightarrow 14\left(\frac{x-7}{3-7}\right) + 12\left(\frac{x-3}{7-3}\right)$$

$$\Rightarrow -14 \times 4^{-1}(x-7) + 12 \cdot 4^{-1}(x-3)$$

$$\Rightarrow 14 \times 13(x-7) + 12 \cdot 13(x-3)$$

$$\Rightarrow -182(x-7) + 156(x-3)$$

$$\Rightarrow -26x + 806 \Rightarrow 8x + 7 \,//$$

#3 & #4 $\overset{x_1\ y_1}{(9, 11)}$ $\overset{x_2\ y_2}{(7, 12)}$

$$L(x) = y_1\left(\frac{x-x_2}{x_1-x_2}\right) + y_2\left(\frac{x-x_1}{x_2-x_1}\right)$$

$$\Rightarrow 11\left(\frac{x-7}{9-7}\right)+12\left(\frac{x-9}{7-9}\right)$$

$2^{-1} \bmod 17 = 9.$

$$\Rightarrow 11 \times 2^{-1}(x-7) - 12 \cdot 2^{-1}(x-9)$$

$$\Rightarrow 99(x-7) - 108(x-9)$$

$$\Rightarrow 99x - 693 - 108x + 972$$

$$\Rightarrow -9x + 279$$

$$\Rightarrow 8x + 7 \,//$$

therefore, #1 (12,2) is dishonest participant.