Exercise 10.1. Consider $f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$.

(a) [1pts] Show that $f(x)$ is irreducible.
(b) [1pts] Let $E = \mathbb{Z}_3[x]/\langle f(x) \rangle$. What is $\chi(E)$?

Solution:

(a) $f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ is irreducible because it does not have zeros in $\mathbb{Z}_3$:

$$f(0) \equiv_3 2 \neq 0 \qquad f(1) \equiv_3 2 \neq 0 \qquad f(2) \equiv_3 1 \neq 0.$$

(b) [1pts] Obviously $\chi(E) = 3$.

□

Exercise 10.2. [10pts] Consider the following elements in $E = \mathbb{Z}_3[x]/\langle x^2 + 2x + 2 \rangle$:

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

(a) Compute the unique representatives for $a \cdot b$ and $a + b$. Don't use any software.
(b) Find c^{-1} in E. Don't use any software.
(c) Compute all distinct powers of a in E. You are allowed to use WolframAlpha for this question.
`PolynomialMod[(2x+1)^5, {3,x^2+2x+2}]`
(d) Find $|a|$ in E^*. Is a primitive in E?
(e) For $\alpha, \beta \in E$ the logarithm $\log_\alpha(\beta)$ of β to the base α is s if $\beta = \alpha^s$. Use the powers from (c) to compute $\log_{2x+1}(2x + 2)$ and $\log_{2x+1}(x + 1)$.
(f) Alice and Bob run the Diffie–Hellman key-exhcnage protocol in the field E using the base element $g = 2x+1$ If the Alice's public key is $A = x$ and Bob's public key is $B = x+1$, then what is their shared secret? In other words, solve the instance $CDH(2x + 1, x, x + 1)$ of the computational Diffie–Hellman problem.

Solution:

(a) $a \cdot b = x + 1$ and $a + b = 0$.
(b) $x(\alpha x+\beta) = \alpha x^2 +\beta x = \alpha(x+1)+\beta x = (\alpha+\beta)x+\alpha = 1$. Hence, $\alpha = 1$ and $\beta = 2$. Therefore, $c^{-1} = x + 2$
(c)

$$(2x + 1)^0 = 1 \qquad (2x + 1)^1 = 2x + 1 \qquad (2x + 1)^2 = 2x + 2 \qquad (2x + 1)^3 = x$$
$$(2x + 1)^4 = 2 \qquad (2x + 1)^5 = x + 2 \qquad (2x + 1)^6 = x + 1 \qquad (2x + 1)^7 = 2x$$
$$(2x + 1)^8 = 1.$$

(d) Clearly $|a| = 8$ and a is primitive.
(e) $\log_{2x+1}(2x + 2) = 2$ and $\log_{2x+1}(x + 1) = 6$.
(f) Since $\log_{2x+1}(x) = 3$ and $\log_{2x+1}(x + 1) = 6$, the shared key must be $(2x + 1)^{3\cdot 6} = (2x + 1)^{18} = (2x + 1)^2 = 2x + 2$.

□

Exercise 10.3. [10pts] Consider a homogeneous system of linear equations with coefficients $\alpha_{ij} \in F$

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

Show that the set of solutions S, i.e., the set

$$\left\{ (x_1, \ldots, x_t) \in F^t \;\middle|\; (x_1, \ldots, x_t) \text{ satisfies the system} \right\}$$

is a subspace of F^t.

Solution: Straightforward check of the axioms of a vector space.

- $(S, +)$ is an abelian group

(a) S contains the trivial element $(0, 0, \ldots, 0)$.
(b) If $(x_1, \ldots, x_t) \in S$, then $-(x_1, \ldots, x_t) \in S$. Hence, S contains inverses.
(c) $+$ is associative on S, because it is associative on the whole space F^t.
(d) $+$ is commutative on S, because it is commutative on the whole space F^t.

- $\alpha(\beta a) = (\alpha\beta)a$ and $1a = a$. Obvious (because the same identitites hold in F^t).
- $(\alpha + \beta)a = \alpha a + \beta a$ and $\alpha(a + b) = \alpha a + \alpha b$. Obvious (because the same identitites hold in F^t).

□

Exercise 10.4. [10pts] Consider a case of the Blakley secret-sharing $(2, 3)$-threshold scheme in which the dealer uses the field $\mathbb{Z}_{17}$ and distributes the following shares:

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

What is the secret?

Solution: Solve the system

$$\begin{cases} 2x_1 + 7x_2 \equiv_{17} 7 \\ 3x_1 + 4x_2 \equiv_{17} 8 \\ -x_1 + 9x_2 \equiv_{17} 0 \end{cases}$$

Using the last equation we get $x_1 \equiv_{17} 9x_2$ and a system

$$\begin{cases} 18x_2 + 7x_2 \equiv_{17} 25x_2 \equiv_{17} 8x_2 \equiv_{17} 7 \\ 27x_2 + 4x_2 \equiv_{17} 31x_2 \equiv_{17} -3x_2 \equiv_{17} 8 \end{cases}$$

But then

$$-3(-3x_2) - (8x_2) = x_2 = (-3)8 - 7 = -31 \equiv_{17} 3.$$

and $x_1 = 3 \cdot 9 = 27 \equiv_{17} = 10$. Therefore, $(10, 3)$ is the secret.

□

Exercise 10.5. [10pts] Use the Lagrange interpolation formula to find a unique quadratic polynomial $f(x) \in \mathbb{R}[x]$ satisfying

- $f(-1) = 1$,
- $f(1) = -1$,
- $f(2) = 4$.

Solution: It is $f(x) = 2x^2 - x - 2$. □

Exercise 10.6. [10pts] Consider an instance of Shamir's $(3, 10)$-threshold scheme over $\mathbb{Z}_{11}$. Suppose that three participants contribute their shares

#1 $(2, 9)$,
#2 $(5, 0)$,
#3 $(8, 7)$,

to compute the secret. Find the secret.

Solution: $f(x) = 7x^2 + 3x + 8$ and the secret is 8. □

Exercise 10.7. [10pts] Consider an instance of Shamir's $(2, 4)$-threshold scheme over $\mathbb{Z}_{17}$. Suppose that all four participants decide to compute the secret and contribute their shares

#1 $(12, 2)$,
#2 $(3, 14)$,
#3 $(9, 11)$,
#4 $(7, 12)$.

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

Solution: In a $(2, n)$-scheme, the function $f(x)$ used to construct shares is linear $mx + b$ and every two participants can reconstruct it. We can use Lagrange interpolation formula to find $f(x)$ for each pair of participants. Or we can reconstruct $m = \frac{y_2 - y_1}{x_2 - x_1}$ for all pairs of participants:

	#1	#2	#3	#4
#1		10	14	15
#2			8	8
#3				8

Here we see that $m = 8$ is consistent for participants #2, #3, and #4. And the share of the participant #1 gives different values of m. Hence, #1 must be dishonest. $\square$