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 $\chi(E)$?

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.

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.

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?

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

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

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.

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.