Homework 1

1. **Practice with Fields.** We shall work over the field $(\mathbb{Z}_7, +, \times)$.

   - (7 points) Addition Table. The (i, j)-th entry in the table is $i + j$. Complete this table. You do not need to fill the black cells because the addition is commutative.

	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Table 1: Addition Table.

   - (7 points) Multiplication Table. The (i, j)-th entry in the table is $i \times j$. Complete this table.

	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Table 2: Multiplication Table.

   - (3.25 points) Additive and Multiplicative Inverses. Write the additive and multiplicative inverses in the table below.

	0	1	2	3	4	5	6
Additive Inverse							
Multiplicative Inverse							

Table 3: Additive and Multiplicative Inverses Table.

- (10.5 points) Division Table. The (i, j)-th entry in the table is i/j. Complete this table.

	1	2	3	4	5	6
0						
1						
2						
3						
4						
5						
6						

Table 4: Division Table.

2. **An Illustrative Execution of Shamir's Secret Sharing Scheme.** We shall work over the field $(\mathbb{Z}_7, +, \times)$. We are interested in sharing a secret among 6 parties such that any 4 parties can reconstruct the secret, but no subset of 3 parties gain any additional information about the secret.

   Suppose the secret is $s = 5$. The random polynomial of degree < 4 that is chosen during the secret sharing steps is $p(X) = 2X^2 + 3X + 5$.

   - (12 points) What are the respective secret shares of parties 1, 2, 3, 4, 5, and 6?
   - (16 points) Suppose parties 1, 3, 5, and 6 are interested in reconstructing the secret. Run Lagrange Interpolation algorithm as explained in the class.

     (*Remark:* It is essential to show the step-wise reconstruction procedure to score full points. In particular, you need to write down the polynomials $p_1(X)$, $p_2(X)$, $p_3(X)$, and $p_4(X)$.)
   - (18 points) Suppose parties 1, 3, and 5 get together. Let $q_{\widetilde{s}}(X)$ be the polynomial that is consistent with their shares and the point $(0, \widetilde{s})$, for each $\widetilde{s} \in \mathbb{Z}_p$. Write down the polynomials $q_0(X)$, $q_1(X)$, $\ldots$, $q_6(X)$.

3. **A bit of Counting.** In this problem, we will do a bit of counting related to polynomials that pass through a given set of points in the plane.

   We are working over the field $(\mathbb{Z}_p, +, \times)$, where p is a prime number. Let $\mathcal{P}_t$ be the set of all polynomials in the indeterminate X with degree $< t$ and coefficients in $\mathbb{Z}_p$.

   - (15 points) Let (x_1, y_1), (x_2, y_2), ..., and (x_t, y_t) be t points in the plane $\mathbb{Z}_p^2$. We have that $x_i \neq x_j$ for all $i \neq j$, that is, the first coordinates of the points are all distinct.

     Prove that there exists a *unique polynomial* in $\mathcal{P}_t$ that passes through these t points.

     (Hint: Use Lagrange Interpolation and Schwartz–Zippel Lemma.)

   - (15 points) Let (x_1, y_1), (x_2, y_2), ..., and (x_{t-1}, y_{t-1}) be $(t-1)$ points in the plane $\mathbb{Z}_p^2$. We have that $x_i \neq x_j$ for all $i \neq j$, that is, the first coordinates of the points are all distinct.

     Prove that there are p polynomials in $\mathcal{P}_t$ that pass through these $(t-1)$ points.

   - (20 points) Let (x_1, y_1), (x_2, y_2), ..., and (x_k, y_k) be k points in the plane $\mathbb{Z}_p^2$, where $k \leqslant t$. We have that $x_i \neq x_j$ for all $i \neq j$, that is, the first coordinates of the points are all distinct.

     Prove that there are p^{t-k} polynomials in $\mathcal{P}_t$ that pass through these k points.

4. **A bit of Probability.** Recall Shamir's secret sharing algorithm. In this problem, we shall prove a few properties of this secret sharing scheme.

   Suppose we are working over the field $(\mathbb{Z}_p, +, \times)$. Let $\mathbb{P}[S = s]$, for $s \in \mathbb{Z}_p$, be the a priori probability of the secret s. We are interested in sharing secrets among n parties such that any t parties can reconstruct the secret, and no additional information about the secret is revealed to any subset of $(t-1)$ parties.

   Let $\mathcal{P}_t$ be the set of all polynomials in the indeterminate X with degree $< t$ and coefficients in $\mathbb{Z}_p$. Let $p(X)$ represent the polynomial used to secret share s. Let s_i represent the evaluation of the polynomial $p(X)$ at $X = i$, represented by $p(i)$, for $i \in \{1, \dots, p-1\}$. That is, the secret share received by party i is s_i.

   - (10 points) For a fixed secret $s \in \mathbb{Z}_p$, prove that

   $$\mathbb{P}\left[p(0) = s\right] = \mathbb{P}[S = s]$$

   - (10 points) For $x_1 \in \mathbb{Z}_p^*$ and $y_1 \in \mathbb{Z}_p$, prove that

   $$\mathbb{P}\left[p(0) = s, p(x_1) = y_1\right] = \frac{\mathbb{P}[S = s]}{p}$$

   - (10 points) For $0 \leqslant k < t$, distinct $x_1, \dots, x_k \in \mathbb{Z}_p^*$ and $y_1, \dots, y_k \in \mathbb{Z}_p$

   $$\mathbb{P}\left[p(0) = s, p(x_1) = y_1, \dots, p(x_k) = y_k\right] = \frac{\mathbb{P}[S = s]}{p^k}$$

   - (10 points) For $0 \leqslant k < t$, distinct $x_1, \dots, x_k \in \mathbb{Z}_p^*$ and $y_1, \dots, y_k \in \mathbb{Z}_p$

   $$\mathbb{P}\left[p(x_1) = y_1, \dots, p(x_k) = y_k\right] = \frac{1}{p^k}$$

5. (36.25 points) **Privacy Concern.** In the class, a few students proposed that we restrict Shamir's Secret Sharing scheme to use only polynomials of degree $(t-1)$ instead of all polynomials of degree $< t$. We will demonstrate a security flaw with this modified scheme.

   Suppose $t = 3$ and we are working over $(\mathbb{Z}_5, +, \times)$. A priori, we have $\mathbb{P}[S = s] = \frac{1}{5}$, for all secrets $s \in \mathbb{Z}_5$. Assume that $p(X) = X^2 + 1$ was the polynomial used for secret sharing.

   Suppose party 1 and party 3 get together. Given their secret shares, what is the a posteriori probability of each secret?