Homework 4

1. **Lagrange Interpolation.** We want to derive a part of the Chinese Remainder Theorem using principles of Lagrange Interpolation. Our goal is the following

> Suppose p and q are two distinct primes. Suppose $a \in \{0, \dots, p-1\}$ and $b \in \{0, \dots, q-1\}$. We want to find a natural number x such that
>
> $$x \pmod p = a \text{ and } x \pmod q = b$$

   (a) (10 points) Find a natural number x_p such that : $x_p \pmod p = 1$ and $x_p \pmod q = 0$.
   Solution.

(b) (12 points) Find a natural number x_q such that : $x_q \pmod{p} = 0$ and $x_q \pmod{q} = 1$.

Solution.

(c) (5 points) Find a natural number x such that : $x \pmod{p} = a$ and $x \pmod{q} = b$.

Solution.

2. **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 $\mathbb{Z}_p$.

   (a) (10 points) Let (x_1, y_1), (x_2, y_2), $\dots$, 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.)

   Solution.

(b) (10 points) Let (x_1, y_1), (x_2, y_2), $\ldots$, 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.

Solution.

(c) (10 points) Let (x_1, y_1), (x_2, y_2), $\ldots$, 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.

Solution.

3. **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 $p(X) = 2X^2 + 3X + 5$.

   (a) (6 points) What are the respective secret shares of parties 1, 2, 3, 4, 5, and 6?
   Solution.

(b) (10 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 $p_4(X)$.)

Solution.

(c) (7 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 $q_0(X)$, $q_1(X)$, $\dots$, $q_6(X)$.
Solution.

4. (20 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?
   Solution.

Collaborators :