Solution of Homework 3

1. **Security of encryption schemes (8+8+8 points).** For each of the encryption schemes below, state whether the scheme is secure or not. Justify your answer in each case.

   (a) The message space is $\mathcal{M} = \{0, 1, \dots, 6\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{1, \dots, 6\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk+m) \mod 7$, and the decryption algorithm $\mathsf{Dec}_{sk}(c)$ returns $(c-sk) \mod 7$.
   Solution.
   According to the Shannon theorem stated in the class, if a private key encryption scheme is correct and secure, then the size of its key space is not smaller than the size of its message space i.e. $|\mathcal{K}| \geqslant |\mathcal{M}|$. The given encryption scheme is correct because

   $$\mathsf{Dec}_{sk}(\mathsf{Enc}_{sk}(m)) = \mathsf{Enc}_{sk}(m) - sk \mod 7 = (((sk+m) \mod 7) - sk) \mod 7 = sk \mod 7.$$

   However, $|\mathcal{K}| = 6$ and $|\mathcal{M}| = 7$ which implies that it is not secure.

(b) The message space is $\mathcal{M} = \{0, 1, \ldots, 6\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, \ldots, 7\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 7$, and the decryption algorithm $\mathsf{Dec}_{sk}(c)$ returns $(c - sk) \mod 7$.

Solution.
We shall use graph representation to prove that the scheme is not secure. Let $c = 6$, $m = 6$ and $m' = 5$. Then, $\mathrm{wt}(m, c) = 2$ because for $\mathsf{sk} \in \{0, 7\}$, we have $\mathsf{Enc}_{sk}(m) = c$. And $\mathrm{wt}(m', c) = 1$ because for only $\mathsf{sk} = 1$, we have $\mathsf{Enc}_{sk}(m') = c$. Since $\mathrm{wt}(m, c) \neq \mathrm{wt}(m', c)$, we conclude that the encryption scheme is not secure.

(c) The message space is $\mathcal{M} = \{1, 3, 5, \dots, 2019, 2021\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 2, 4, 6, \dots, 2020\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 2022$, and the decryption algorithm $\mathsf{Dec}_{sk}(c)$ returns $(c - sk) \mod 2022$.

Solution.

We shall use graph representation to prove that the scheme is secure. The message space is the set of odd integers less than 2021 and the key space is the set of even integers less than 2022 and the summation of an even and an odd integer modulo 2022 is an odd integer. Thus, the cipher text space is $\mathcal{C} = \{1, 3, 5, \dots, 2021\}$.

Let $c = 2j - 1$ for some j in the set $\{1, 2, \dots, 1011\}$ and $m = 2i - 1$ for some $i \in \{1, 2, \dots, 1011\}$. Then, $\mathrm{wt}(m, c) = 1$ because the only key $\mathsf{sk} \in \mathcal{K}$ for which $\mathsf{Enc}_{sk}(m) = c$ is $\mathrm{sk} = 2(j - i) \mod 2022$ (if $j \geqslant i$ then $2(j - i)$ is the key and if $j < i$, then $2(j - i) + 2022$ is the key) which is an even integer less than 2022 and the key space contains that(note that this is important to make sure that this key exists in the key space). Since for each m and c, $\mathrm{wt}(m, c) = 1$, the encryption scheme is secure.

2. **Equivalent definition of Perfect Secrecy (15 points).** In the lecture we defined the perfect security for any private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows. For any message m, cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{M} = m | \mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{M} = m\right]$$

Show that the above definition is equivalent to the following alternative definition. For all messages m, m', cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m\right] = \mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m'\right],$$

Remarks: (1) Proving equivalence means that you have to show that the first definition implies the second definition. And, the second definition also implies the first definition.

(2) Additionally, in this problem, for simplicity, assume that in the the probability expressions no "division by error" occurs.

Solution.
Forward direction : We are given that for any message m, cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{M} = m | \mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{M} = m\right]$$

We can use Baye's rule to do the following manipulation :

$$\begin{aligned}
\Pr[\mathbb{M} = m | \mathbb{C} = c] &= \Pr[\mathbb{M} = m] \\
\frac{\Pr[\mathbb{M} = m, \mathbb{C} = c]}{\Pr[\mathbb{C} = c]} &= \Pr[\mathbb{M} = m] \\
\frac{\Pr[\mathbb{M} = m, \mathbb{C} = c]}{\Pr[\mathbb{M} = m]} &= \Pr[\mathbb{C} = c] \\
\Pr[\mathbb{C} = c | \mathbb{M} = m] &= \Pr[\mathbb{C} = c]
\end{aligned}$$

Since the RHS is independent of $\mathbb{M} = m$, the above expression must be true for any $\mathbb{M} = m$, so we can write $\Pr[\mathbb{C} = c | \mathbb{M} = m'] = \Pr[\mathbb{C} = c]$. Therefore we have that $\Pr[\mathbb{C} = c | \mathbb{M} = m] = \Pr[\mathbb{C} = c | \mathbb{M} = m']$.
Backward direction : We are given that for all messages m, m', cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m\right] = \mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m'\right] = \alpha \text{ (say)}$$

Observe that

$$\begin{aligned}
\Pr[\mathbb{C}=c] &= \sum_{m\in\mathcal{M}} \Pr[\mathbb{C}=c,\mathbb{M}=m] \\
&= \sum_{m\in\mathcal{M}} \Pr[\mathbb{C}=c|\mathbb{M}=m]\Pr[\mathbb{M}=m] \\
&= \sum_{m\in\mathcal{M}} \alpha\Pr[\mathbb{M}=m] \\
&= \alpha\sum_{m\in\mathcal{M}} \Pr[\mathbb{M}=m] \\
&= \alpha\times 1 = \alpha \qquad (1)
\end{aligned}$$

Consider the LHS of the expression that we have to prove

$$\begin{aligned}
\Pr[\mathbb{M}=m|\mathbb{C}=c] &= \frac{\Pr[\mathbb{M}=m,\mathbb{C}=c]}{\Pr[\mathbb{C}=c]} \\
&= \frac{\Pr[\mathbb{C}=c|\mathbb{M}=m]\Pr[\mathbb{M}=m]}{\Pr[\mathbb{C}=c]} \\
&= \frac{\alpha\Pr[\mathbb{M}=m]}{\alpha} \\
&= \Pr[\mathbb{M}=m]
\end{aligned}$$

3. **Defining Perfect Security from Ciphertexts (15 points).** An upstart in the field of cryptography has proposed a new definition for perfect security of private-key encryption schemes. According to this new definition, a private-key encryption scheme (Gen, Enc, Dec) is perfectly secure, if, for all a priori distribution $\mathbb{M}$ over the message space, and any two cipher-texts c and c', we have the following identity.

$$\mathbb{P}\left[\mathbb{C}=c\right]=\mathbb{P}\left[\mathbb{C}=c'\right]$$

Show that the definition in the class does not imply this new definition.

Remark. You need to construct a private-key encryption scheme that is secure according to the definition we learned in the class. However, this scheme does not satisfy the new definition.

Solution.

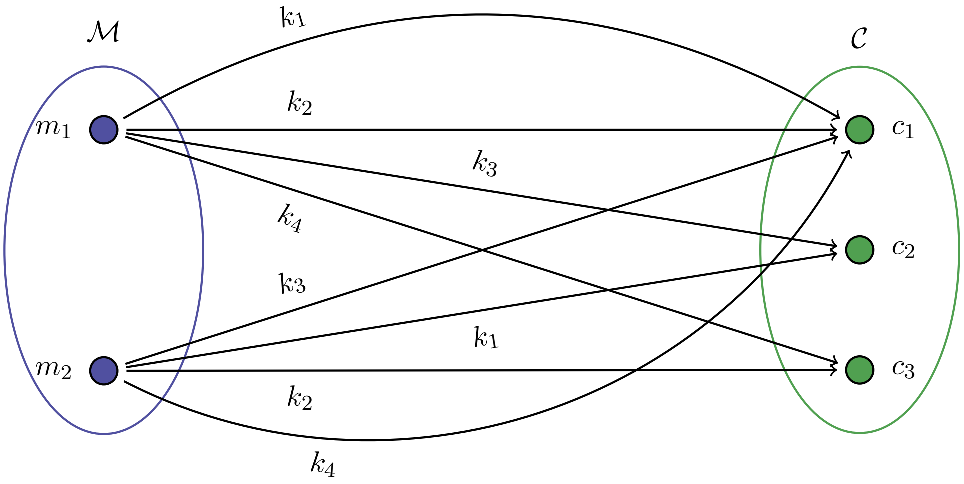

Figure 1: Corresponding graph of encryption scheme Π

Let $\Pi=(\mathsf{Gen},\mathsf{Enc},\mathsf{Dec})$ denote the encryption scheme defined on message space $\mathcal{M}=\{m_1,m_2\}$ such that encryption algorithm Gen chooses a key from set $\{k_1,k_2,k_3,k_4\}$ uniformly at random and the ciphertext space is defined as $\mathcal{C}:=\{c_1,c_2,c_3\}$. Encryption scheme is defined in the following table.

	m_1	m_2
k_1	c_1	c_2
k_2	c_1	c_3
k_3	c_2	c_1
k_4	c_3	c_1

The corresponding graph for encryption scheme Π is given in figure 1.

We have

$$\Pr[\mathbb{C} = c_1 | \mathbb{M} = m_1] = \Pr[\mathbb{K} \in \{k_1, k_2\} | \mathbb{M} = m_1] = \Pr[\mathbb{K} \in \{k_1, k_2\}] = \frac{2}{4} = \frac{1}{2}$$

$$\Pr[\mathbb{C} = c_1 | \mathbb{M} = m_2] = \Pr[\mathbb{K} \in \{k_3, k_4\} | \mathbb{M} = m_2] = \Pr[\mathbb{K} \in \{k_3, k_4\}] = \frac{2}{4} = \frac{1}{2}$$

$$\Pr[\mathbb{C} = c_2 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_3 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_3] = \frac{1}{4}$$

$$\Pr[\mathbb{C} = c_2 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_1 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_1] = \frac{1}{4}$$

$$\Pr[\mathbb{C} = c_3 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_4 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_4] = \frac{1}{4}$$

$$\Pr[\mathbb{C} = c_3 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_2 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_2] = \frac{1}{4}$$

Therefore, for any $c \in \mathcal{C}$, we have $\Pr[\mathbb{C} = c | \mathbb{M} = m_1] = \Pr[\mathbb{C} = c | \mathbb{M} = m_2]$ which according to question 1, implies that $\Pr[\mathbb{M} = m | \mathbb{C} = c] = \Pr[\mathbb{M} = m]$ for any chipertext c, any message m and any probability distribution $\mathbb{M}$ over message space. Note that if we want to prove $\Pr[\mathbb{M} = m | \mathbb{C} = c] = \Pr[\mathbb{M} = m]$ directly, then we need to prove it for any arbitrary probability distribution $\mathbb{M}$ not only uniform distribution. However,we have:

$$\Pr[\mathbb{C} = c_1] = \Pr[\mathbb{C} = c_1 | \mathbb{M} = m_1] \Pr[\mathbb{M} = m_1] + \Pr[\mathbb{C} = c_1 | \mathbb{M} = m_2] \Pr[\mathbb{M} = m_2] \tag{2}$$

$$= \frac{1}{2} \times \Pr[\mathbb{M} = m_1] + \frac{1}{2} \times \Pr[\mathbb{M} = m_2] = \frac{1}{2} \tag{3}$$

and

$$\Pr[\mathbb{C} = c_2] = \Pr[\mathbb{C} = c_2 | \mathbb{M} = m_1] \Pr[\mathbb{M} = m_1] + \Pr[\mathbb{C} = c_2 | \mathbb{M} = m_2] \Pr[\mathbb{M} = m_2] \tag{4}$$

$$= \frac{1}{4} \times \Pr[\mathbb{M} = m_1] + \frac{1}{4} \times \Pr[\mathbb{M} = m_2] = \frac{1}{4} \tag{5}$$

So, $\Pr[\mathbb{C} = c_1] \neq \Pr[\mathbb{C} = c_2]$ which means that the definition in the class does not imply the definition introduced in the question.

4. **One-time Pad for 4-Alphabet Words (8+8 points).** We interpret alphabets $\mathtt{a}, \mathtt{b}, \dots, \mathtt{z}$ as integers $0, 1, \dots, 25$, respectively. We will work over the group $(\mathbb{Z}_{26}^4, +)$, where $+$ is coordinate-wise integer sum $\mod 26$. For example, $\mathtt{abcx} + \mathtt{aczd} = \mathtt{adba}$.

   Now, consider the one-time pad encryption scheme over the group $(\mathbb{Z}_{26}^4, +)$.

   (a) What is the probability that the encryption of the message `kiwi` is the cipher text `kiwi`?
   Solution.

$$\begin{aligned}\Pr[\mathsf{Enc}_{\mathsf{sk}}(\mathtt{kiwi}) = \mathtt{kiwi}] &= \Pr[\mathbb{C} = \mathtt{kiwi} | \mathbb{M} = \mathtt{kiwi}] \\ &= \Pr[\mathbb{SK} = aaaa | \mathbb{M} = \mathtt{kiwi}] \\ &= \Pr[\mathbb{SK} = aaaa] \quad \text{(key is chosen independent of message)} \\ &= \frac{1}{26^4} \quad \text{(key is chosen uniformly at random)}\end{aligned}$$

   Note. Since the secret key is drawn uniformly at random, for $\mathbb{SK} = sk_1 sk_2 sk_3 sk_4$, $\Pr[\mathbb{SK} = aaaa] = \Pr[sk_1 = a, sk_2 = a, sk_3 = a, sk_4 = a] = \Pr[sk_1 = a] \times \Pr[sk_2 = a] \times \Pr[sk_3 = a] \times \Pr[sk_4 = a] = \frac{1}{26} \cdot \frac{1}{26} \cdot \frac{1}{26} \cdot \frac{1}{26}$.

   (b) What is the probability that the encryption of the message `kiwi` is the cipher text `lime`?
   Solution.

$$\begin{aligned}\Pr[\mathsf{Enc}_{\mathsf{sk}}(\mathtt{kiwi}) = \mathtt{lime}] &= \Pr[\mathbb{C} = \mathtt{lime} | \mathbb{M} = \mathtt{kiwi}] \\ &= \Pr[\mathbb{SK} = \mathrm{baqw} | \mathbb{M} = \mathtt{kiwi}] \\ &= \Pr[\mathbb{SK} = \mathrm{baqw}] \quad \text{(key is chosen independent of message)} \\ &= \frac{1}{26^4} \quad \text{(key is chosen uniformly at random)}\end{aligned}$$

5. **Lagrange Interpolation(7+7+6 points).** 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
>
> $$x \pmod p = a \text{ and } x \pmod q = b$$

We shall proceed towards this objective incrementally (similar to the approach of Lagrange interpolation).

(a) Find a natural number x_p satisfying $x_p \pmod p = 1$, and $x_p \pmod q = 0$.
Solution.
In order for x_p to satisfy $x_p \pmod q = 0$, we know it has to be a multiple of q. Furthermore, using the result from Homework 2, we know that $x^{p-1} = 1 \mod p$, for any integer x that is not divisible by p. So, one value of x that we can choose is q (because p and q are distinct primes). Therefore, $x_p = q^{p-1}$ simultaneously satisfies $x_p = 0 \mod q$ and $x_p = 1 \mod p$.

(b) Find a natural number x_q satisfying $x_q \pmod{p} = 0$ and $x_q \pmod{q} = 1$.
Solution.
Similar to part (a) of our solution, we conclude that $x_q = p^{q-1}$ satisfies $x_q = 0 \mod p$ and $x_q = 1 \mod q$.

(c) Find a natural number x satisfying $x \pmod p = a$ and $x \pmod q = b$.
Solution.
We use parts (a) and (b) to claim that $x = ax_p + bx_q$ satisfies

$$x \mod p = ax_p \mod p + bx_q \mod p = a \times 1 + b \times 0 = a \mod p$$

and

$$x \mod q = ax_p \mod q + bx_q \mod q = a \times 0 + b \times 1 = b \mod q.$$

6. **An Illustrative Execution of Shamir's Secret Sharing Scheme (6+10+9 points).** 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 $s = 3$. The random polynomial of degree < 4 that is chosen during the secret sharing steps is $p(X) = X^3 + 2X + 3$.

   (a) What are the respective secret shares of parties 1, 2, 3, 4, 5, and 6?
   Solution.
   Recall that the secret share of party i is the evaluation of the polynomial $p(X)$ at $X = i$. Therefore, the secret shares of parties $1, 2, 3, 4, 5, 6$ are $6, 1, 1, 5, 5, 0$, respectively. We calculate one of them as an example:

$$p(3) \mod 7 = 3^3 + 2 \times 3 + 3 \mod 7 = 6 + 6 + 3 \mod 7 = 1$$

(b) Suppose parties 1, 2, 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.

We want to construct a polynomial of degree at most 3 that passes through 4 points $(x_1, y_1) = (1, 6), (x_2, y_2) = (2, 1), (x_3, y_3) = (5, 5), (x_4, y_4) = (6, 0)$.

The sub-problem i is to construct a polynomial $p_i(X)$ of degree at most 3 that passes through (x_i, y_i) and $(x_j, 0)$ where $j \neq i$. The following is the the formula of the polynomial $p_i(X)$.

$$p_i(X) = y_i \cdot \prod_{j \neq i} \frac{(X - x_j)}{(x_i - x_j)} = c_i \cdot \prod_{j \neq i} (X - x_j)$$

where $c_i \cdot \prod_{j \neq i}(x_i - x_j) = y_i \mod 7$.

i. Sub-problem 1: $c_1 \cdot (1-2)(1-5)(1-6) = 6 \mod 7$, which implies $c_1 = 6$. Thus $p_1(X) = 6(X-2)(X-5)(X-6)$.

ii. Sub-problem 2: $c_2 \cdot (2-1)(2-5)(2-6) = 1 \mod 7$, which implies $c_2 = 3$. Thus $p_1(X) = 3(X-1)(X-5)(X-6)$.

iii. Sub-problem 3: $c_3 \cdot (5-1)(5-2)(5-6) = 5 \mod 7$, which implies $c_3 = 6$. Thus $p_1(X) = 6(X-1)(X-2)(X-6)$.

iv. Sub-problem 4: $c_4 \cdot (6-1)(6-2)(6-5) = 0 \mod 7$, which implies $c_4 = 0$. Thus $p_1(X) = 0 \times (X-1)(X-2)(X-5) = 0$.

Therefore, we have

$$p(X) = p_1(X) + p_2(X) + p_3(X) + p_4(X) = X^3 + 2X + 3.$$

(c) Suppose parties 1, 2, 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 $q_0(X)$, $q_1(X)$, …, $q_6(X)$.
Solution.

Note that the polynomial, for $\widetilde{z} \in \mathbb{Z}_7$, is

$$q_{\widetilde{s}}(X) = c_{\widetilde{s}}(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) \text{ such that } q_{\widetilde{s}}(0) = \widetilde{s}$$

where the following constraints are satisfied for the polynomials $\alpha(X), \beta(X)$, and $\gamma(X)$.

$$\begin{aligned}
\alpha(X) &= c_1X(X-2)(X-5) \text{ such that } \alpha(1) = 6\\
\beta(X) &= c_2X(X-1)(X-5) \text{ such that } \beta(2) = 1\\
\gamma(X) &= c_3X(X-1)(X-2) \text{ such that } \gamma(5) = 5
\end{aligned}$$

Solving, we get $\alpha(X) = 5X(X-2)(X-5)$, $\beta(X) = X(X-1)(X-5)$, and $\gamma(X) = 3X(X-1)(X-2)$. Since $q_{\widetilde{s}}(0) = \widetilde{s}$, we can find $c_{\widetilde{s}}$ using the following equation

$$c_{\widetilde{s}} \cdot (-10) = c_{\widetilde{s}} \cdot 4 = \widetilde{s} \mod 7 \text{ for every } \widetilde{s} \in \mathbb{Z}_7.$$

Therefore, we have

$$\begin{aligned}
q_0(X) &= 0(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = 2X^3 + 6X^2 + 5X\\
q_1(X) &= 2(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = 4X^3 + 4X^2 + 4X + 1\\
q_2(X) &= 4(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = 6X^3 + 2X^2 + 3X + 2\\
q_3(X) &= 6(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = X^3 + 2X + 3\\
q_4(X) &= 1(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = 3X^3 + 5X^2 + X + 4\\
q_5(X) &= 3(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = 5X^3 + 3X^2 + 5\\
q_6(X) &= 5(X-1)(X-2)(X-5) + \alpha(X) + \beta(X) + \gamma(X) = X^2 + 6X + 6
\end{aligned}$$

7. **A bit of Counting (8+8+9 points).** 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 already did this counting (slightly informally) in the class. Writing the solution for this problem shall make the solution's intuition more concrete.

   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) 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.)

   Solution.

   Lagrange Interpolation demonstrates that there is at least one polynomial passing through these points that has degree at most $(t-1)$.

   Now, we want to show that there is at most one polynomial passing through these points. We shall prove this by contradiction. Assume that there are two distinct polynomials $A(X)$ and $B(X)$ of degree $< t$ such that both pass through all these points. Therefore, the polynomial $C(X) := A(X) - B(X)$ is not the zero polynomial (because $A(X)$ and $B(X)$ are distinct). Simultaneously, the polynomial $C(X)$ has $\{x_1, x_2, \ldots, x_t\}$ as its roots. By Schwartz–Zippel Lemma, the polynomial $C(X)$ must be the zero polynomial (because it has t roots and degree $< t$). Hence, contradiction.

(b) Let (x_1, y_1), (x_2, y_2), $\dots$, 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.
Let x_t be distinct from $\{x_1, \dots, x_{t-1}\}$. Using part (a) of the result, there exists a unique polynomial passing through

$$\{(x_1, y_1), (x_2, y_2), \dots, (x_{t-1}, y_{t-1}), (x_t, 0)\}$$

Similarly, there exists a unique polynomial passing through

$$\{(x_1, y_1), (x_2, y_2), \dots, (x_{t-1}, y_{t-1}), (x_t, 1)\}$$

And this polynomial is different from the previous one (because they evaluate to different values at x_t).
Similarly, there exists a unique polynomial passing through

$$\{(x_1, y_1), (x_2, y_2), \dots, (x_{t-1}, y_{t-1}), (x_t, 2)\}$$

that is different from all previous ones.
And so on...
Formally, we argue as follows. Considering each value of $y \in \{0, 1, \dots, p-1\}$, we obtain a distinct polynomial that passes through the points

$$\{(x_1, y_1), (x_2, y_2), \dots, (x_{t-1}, y_{t-1}), (x_t, y)\}$$

So, a total of p polynomials pass through

$$\{(x_1, y_1), (x_2, y_2), \dots, (x_{t-1}, y_{t-1})\}$$

(c) Let (x_1, y_1), (x_2, y_2), $\dots$, 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. a similar counting argument as in part (b), consider the points

$$(x_1, y_1), \dots, (x_k, y_k), (x_{k+1}, r_1), \dots, (x_t, r_{t-k})$$

Where the first coordinates are all distinct from each other. Since each $r_i \in \{r_1, \dots r_{t-k}\}$ can take p values ($\{0, 1, \dots, p-1\}$), we obtain p^{t-k} polynomials.

Collaborators :