1. **How many polynomials?**

Let $P(x)$ be a polynomial of degree 2 over GF(5). As we saw in lecture, we need $d + 1$ distinct points to determine a unique $d$-degree polynomial.

1. Assume that we know $P(0) = 1$, and $P(1) = 2$. Now we consider $P(2)$. How many values can $P(2)$ have? List all possible polynomials of degree 2. How many distinct polynomials are there?

2. Now assume that we only know $P(0) = 1$. We consider $P(1)$, and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many different polynomials are there?

3. How many different polynomials of degree $d$ over $GF(p)$ are there if we only know $k$, where $k \leq d$, values?

2. **Where’s my message?**

Alice wants to send the message $(a_0, a_1, a_2)$ to Bob, where each $a_i \in \{0, 1, 2, 3, 4\}$. She encodes it as a polynomial $P$ of degree $\leq 2$ over $GF(5)$ such that $P(0) = a_0$, $P(1) = a_1$, and $P(2) = a_2$, and she sends the packets $(0, P(0))$, $(1, P(1))$, $(2, P(2))$, $(3, P(3))$, $(4, P(4))$. Two packets are dropped, and Bob only learns that $P(0) = 4$, $P(3) = 1$, and $P(4) = 2$. Help Bob recover Alice’s message!

1. Can Bob recover Alice’s message? Why?

2. Recover the message using Lagrange Interpolation.

3. **Lagrange or Linear System**

In this exercise we will try to find out a polynomial $P(x)$ of degree at most 2 with coefficients in $0, \ldots, 4$ such that $P(1) = 2 \pmod{5}$, $P(2) = 4 \pmod{5}$, and $P(3) = 3 \pmod{5}$.

1. Find out the polynomials $\Delta_i(x)$ for $i \in \{1, 2, 3\}$.

2. Combine $\Delta_i$’s with the right coefficients to find the polynomial $P(x)$.

3. Now we will try a different approach. Write the polynomial $P(x)$ as $c_0 + c_1x + c_2x^2$. Treating $c_i$’s as variables what do the equations $P(1) = 2 \pmod{5}$, $P(2) = 4 \pmod{5}$, and $P(3) = 3 \pmod{5}$ tell about $c_i$’s?

4. Solve the system of equations you get from the last part to solve for $c_i$’s. What is the resulting polynomial $P(x)$?