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.

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

Solution: 5 polynomials, each for different values of $P(2)$.

(b) 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? **Solution:** Now there are 5^2 different polynomials.

(c) How many different polynomials of degree d over $GF(p)$ are there if we only know k values, where $k \leq d$? **Solution:** p^{d+1-k} different polynomials. For $k = d+1$, there should only be 1 polynomial.

2. **Lagrange Interpolation**

Find a unique real polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ using Lagrange interpolation.

(a) Find $\Delta_{-1}(x)$ where $\Delta_{-1}(0) = \Delta_{-1}(1) = \Delta_{-1}(2) = 0$ and $\Delta_{-1}(-1) = 1$.

Solution: $\Delta_{-1}(x) = \frac{x(x-1)(x-2)}{-6}$

(b) Find $\Delta_0(x)$ where $\Delta_0(-1) = \Delta_0(1) = \Delta_0(2) = 0$ and $\Delta_0(0) = 1$.

Solution: $\Delta_0(x) = \frac{(x+1)(x-1)(x-2)}{2}$

(c) Find $\Delta_1(x)$ where $\Delta_1(-1) = \Delta_1(0) = \Delta_1(2) = 0$ and $\Delta_1(1) = 1$.

Solution: $\Delta_1(x) = \frac{(x+1)(x)(x-2)}{-2}$.

(d) Find $\Delta_2(x)$ where $\Delta_2(-1) = \Delta_2(0) = \Delta_2(1) = 0$ and $\Delta_2(2) = 1$.

Solution: $\Delta_2(x) = \frac{(x+1)(x)(x-1)}{6}$.

(e) Reconstruct $p(x)$ by using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$ and $\Delta_2(x)$. **Solution:** We don't need $\Delta_2(x)$.

$$\begin{aligned} p(x) &= 3 \cdot \Delta_{-1}(x) + 1 \cdot \Delta_0(x) + 2 \cdot \Delta_1(x) + 0 \cdot \Delta_2(x) \\ &= -\frac{1}{2}x(x-1)(x-2) + \frac{1}{2}(x+1)(x-1)(x-2) + (-1)x(x+1)(x-2) \\ &= -x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + 1 \end{aligned}$$

3. **Secret Sharing**

   Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

   - Both TAs should be able to access the answers
   - All 3 Readers can also access the answers
   - One TA and one Reader should also be able to do the same

   Design a Secret Sharing scheme to make this work.

   Solution: Use a degree 2 polynomial and requires at least 3 shares to recover the polynomial. Generate a total of 7 shares, give each Reader a share, and each TA 2 shares. Then, all possible combinations will have at least 3 shares to recover the answer key.

   Basically, the point of this problem is to assign different weight to different class of people. If we give one share to everyone, then 2 Readers can also recover the secret and the scheme is broken.

4. **Secrets in the United Nations**

   The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination s. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

   (a) Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

   Solution: Create a polynomial of degree $n-1$ and give each country one point. Give the Secretary General $n-m$ points, so that if he collaborates with m countries, they will have $n-m+m=n$ points and can reconstruct the polynomial. Without the General, n countries can come together and also recover the polynomial. No combination of the General with fewer than m countries can recover the polynomial.

   Alternatively:

   Have two schemes, one for the first condition and one for the second.

   For the first condition: just one polynomial of degree $\leq n-1$ would do, where each country gets one point. The polynomial evaluated at 0 would give the secret.

   For the second condition: one polynomial is created of degree $m-1$ and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the secretary general and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

   (b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.

Solution:

The scheme in part (a) remains the same, but instead of directly giving each country a point on the $n-1$ degree polynomial to open the vault, construct an additional polynomial for each country that will produce that point.

Each country's polynomial is degree-$k-1$, and a point is given to each of the k representatives of the country. Thus, when they all get together they can produce a point for either of the schemes.

5. **Sanity check!**

(a) Alice wants to send a message of length 10 to Bob over a lossy channel. What is the degree of the unique polynomial she should use to encode her message?

Solution: 9

(b) Alice sent Bob the values of the above polynomial at 16 distinct points. How many erasure errors can Bob recover from? **Solution:** 6

(c) How many general errors can Bob recover from? **Solution:** 3