1. **Polynomial Intersections**

   Polynomial intersections Find (and prove) an upper-bound on the number of times two distinct degree d polynomials can intersect. What if the polynomialsâĂŹ degrees differ?

2. **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?

   (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?

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

3. **Remainder Riddles**

   There exists a polynomial (over $GF(7)$) $p(x)$ that has a remainder of 3 when divided by $x-1$, a remainder of 1 when divided by $x+1$, and a remainder of $2x+1$ when divided by $x^2-1$.

   Mark one: **TRUE** or **FALSE**.

4. **Secret Sharing**

   Prof. Seshia would like to share a secret number $s$ among us, where $s$ could be any integer from 0 to 10. He chose a polynomial with degree 1 such that $P(0) \equiv s \pmod{11}$, but he only shared $P(1)$ with your GSI. Another key is on your hands. The way he distributed the second key $w = P(2)$ $(0 \leq w \leq 58)$ is by choosing a polynomial $Q(x)$ of degree $\leq 2$ such that $Q(0) \equiv w \pmod{59}$. Here are your $x$ and $Q(x)$:

   (a) At least how many students would we need in order to find $w$?

   (b) Please find $w$.

   (c) Please help your GSI find the secret number $s$.

5. **Berlekamp–Welch algorithm**

   In this question we will go through an example of error-correcting codes with general errors. We will send a message $(m_0, m_1, m_2)$ of length $n = 3$. We will use an error-correcting code for $k = 1$ general error, doing arithmetic modulo 5.

(a) Suppose $(m_0, m_1, m_2) = (4, 3, 2)$. Use Lagrange interpolation to construct a polynomial $P(x)$ of degree 2 (remember all arithmetic is $\bmod 5$) so that $(P(0), P(1), P(2)) = (m_0, m_1, m_2)$. Then extend the message to lengeth $n+2k$ by appending $P(3), P(4)$. What is the polynomial $P(x)$ and what is the message $(c_0, c_1, c_2, c_3, c_4) = (P(0), P(1), P(2), P(3), P(4))$ that is sent?

(b) Suppose the message is corrupted by changing $c_0$ to 0. We will locate the error using the Berlekamp–Welsh method. Let $E(x) = x + b_0$ be the error-locator polynomial, and $Q(x) = P(x)E(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ be a polynomial with unknown coefficients. Write down the system of linear equations (involving unknowns $a_0, a_1, a_2, a_3, b_0$) in the Berlekamp–Welsh method. You need not solve the equations.

(c) The solution to the equations in part (b) is $b_0 = 0, a_0 = 0, a_1 = 4, a_2 = 4, a_3 = 0$. Show how the recipient can recover the original message $(m_0, m_1, m_2)$.