1. **Erasure warm-up**

Working over $GF(q)$, you want to send your friend a message of $n = 4$ packets and guard against 2 lost packets. What is the minimum $q$ you can use? What is the maximum degree of the unique polynomial that describes your message?

2. **Visualizing error correction**

Alice wants to send a message of 2 packets to Bob, and wants to guard against 1 lost packet. So working over $GF(3)$, she finds the unique polynomial $P(x)$ that passes through the points she wants to send, and sends Bob her augmented message of 3 packets: $(0, P(0)), (1, P(1)), (2, P(2))$.

One packet is lost, so Bob receives the following packets: $(0, 2), (2, 0)$.

(a) Plot the points represented by the packets Bob received on the grid below.

(b) Draw in the unique polynomial $P(x)$ that connects these two points.

(c) By visual inspection, find the lost packet $(1, P(1))$.

3. **Where are my packets?**

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.

(a) Find the multiplicative inverses of 1, 2, 3 and 4 modulo 5.
(b) Find the original polynomial $P$ by using Lagrange interpolation or by solving a system of linear equations.

(c) Recover Alice’s original message.

4. More erasures!
Consider the alphabet $A = 0, B = 1, C = 2, D = 3, E = 4$. Suppose a message of length 3 is sent using the error correction scheme discussed in class over $GF(5)$. If you receive the following packets, what was the original message?

(a) $C _ A A$

(b) $A C C$

(c) Can you determine the original message if you only receive $C E _ _$? Either find the original message or explain why you can’t.

5. Polynomial divisibility
Let $A(x), B(x), Q(x),$ and $R(x)$ be 4 polynomials, where $A(x) = B(x)Q(x) + R(x)$, with $0 \leq \deg R(x) < \deg B(x) \leq \deg A(x)$.

Prove that a polynomial $C(x)$ divides $A(x)$ and $B(x)$ if and only if it divides $B(x)$ and $R(x)$. 