CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Dinh, Psomas, and Ye Discussion 7D

1. Roots

Let's make sure you're comfortable with thinking about roots of polynomials in familiar old $\mathbb{R}$. For all of these questions, take the context to be $\mathbb{R}$:

1. True or False: if $p(x) = ax^2 + bx + c$ has two positive roots, then $ab < 0$ and $ac > 0$. Argue why or provide a counterexample.

2. Suppose $P(x)$ and $Q(x)$ are two different nonzero polynomials with degrees d_1 and d_2 respectively. What can you say about the number of solutions of $P(x) = Q(x)$? How about $P(x) \cdot Q(x) = 0$?

3. We've given a lot of attention to the fact that a nonzero polynomial of degree d can have at most d roots. Well, I'm sick of it. What I want to know is, what is the *minimal* number of real roots that a nonzero polynomial of degree d can have? How does the answer depend on d?

4. Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that, if f has exactly one root, then $a^2 = 4b$.

2. Roots: The Next Generations

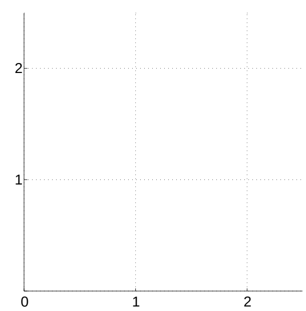
Now go back and do it all over in modular arithmetic...

Which of the facts from above stay true when $\mathbb{R}$ is replaced by $GF(p)$ [i.e., integer arithmetic modulo the prime p]? Which change, and how? Which statements won't even make sense anymore?

3. 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: $(0,2),(2,0)$.

1. Plot the points represented by the packets Bob received on the grid below.



2. Draw in the unique polynomial $P(x)$ that connects these two points.
3. By visual inspection, find the lost packet $(1,P(1))$.

4. 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 ≤ 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. Find the multiplicative inverses of $1,2,3$ and 4 modulo 5.

2. Find the original polynomial P by using Lagrange interpolation or by solving a system of linear equations.

5. 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.

1. 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.

2. 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.