# CS 70 Discrete Mathematics and Probability Theory
# Summer 2015 Chung-Wei Lin Discussion 3B

**1. Roots: The Next Generations**

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

(a) 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.

(b) 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 $P(x) \cdot Q(x) = 0$?

(c) 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 $d$?

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

Which of the facts from above stay true when considering mod $p$ (*i.e.*, integer arithmetic modulo the prime $p$)? Which change, and how? Which statements won't even make sense anymore?

**2. Lagrange Interpolation in Finite Field**

Find a unique polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ in modulo 5 arithmetic using the Lagrange interpolation.

(a) Find $\Delta_{-1}(x)$ where $\Delta_{-1}(0) \equiv \Delta_{-1}(1) \equiv \Delta_{-1}(2) \equiv 0 \pmod 5$ and $\Delta_{-1}(-1) \equiv 1 \pmod 5$.

(b) Find $\Delta_0(x)$ where $\Delta_0(-1) \equiv \Delta_0(1) \equiv \Delta_0(2) \equiv 0 \pmod 5$ and $\Delta_0(0) \equiv 1 \pmod 5$.

(c) Find $\Delta_1(x)$ where $\Delta_1(-1) \equiv \Delta_1(0) \equiv \Delta_1(2) \equiv 0 \pmod 5$ and $\Delta_1(1) \equiv 1 \pmod 5$.

(d) Find $\Delta_2(x)$ where $\Delta_2(-1) \equiv \Delta_2(0) \equiv \Delta_2(1) \equiv 0 \pmod 5$ and $\Delta_2(2) \equiv 1 \pmod 5$.

(e) Construct $p(x)$ using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$, and $\Delta_2(x)$.

## 3. 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? List all possible polynomials of degree 2. 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 $k$, where $k \leq d$, values?

## 4. Secret Sharing

Steven would like to share a secret number $s$ among us, with $s$ 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 $P(1)$ to your TA. 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 TA find the secret number $s$.

## 5. Secret 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.

(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.