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?

It no longer makes sense to discuss positive vs. negative when considering mod p, so (a) above becomes nonsense. The upper bounds on the number of roots in (b) are still true, so do the fact in (d). For (c), even degree polynomials can still have 0 roots, for example $x^2 + 1 \pmod 3$ (or similar FLT-inspired forms). However, we lose the guarantee that every odd degree polynomial must have a root (though we are still assured of this at degree 1). For example, $x^3 + x + 1 \pmod 5$ has no roots.

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 $\Delta_{-1}(-1) \equiv 1 \pmod 5$.
$\Delta_{-1}(x) \equiv x(x-1)(x-2)(-6)^{-1} \equiv 4x(x-1)(x-2) \pmod 5$

(b) Find $\Delta_0(x)$ where $\Delta_0(-1) \equiv \Delta_0(1) \equiv \Delta_0(2) \equiv 0 \pmod 5$ and $\Delta_0(0) \equiv 1 \pmod 5$.
$\Delta_0(x) \equiv (x+1)(x-1)(x-2)(2)^{-1} \equiv 3(x+1)(x-1)(x-2) \pmod 5$

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

(d) Find $\Delta_2(x)$ where $\Delta_2(-1) \equiv \Delta_2(0) \equiv \Delta_2(1) \equiv 0 \pmod 5$ and $\Delta_2(2) \equiv 1 \pmod 5$.
$\Delta_2(x) \equiv (x+1)(x)(x-1)(6)^{-1} \equiv (x+1)(x)(x-1) \pmod 5$.

(e) Construct $p(x)$ using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$, and $\Delta_2(x)$.
We don't need $\Delta_2(x)$. $p(x) \equiv 3 \cdot \Delta_{-1}(x) + 1 \cdot \Delta_0(x) + 2 \cdot \Delta_1(x) + 0 \cdot \Delta_2(x) \equiv 4x^3 + 4x^2 + 3x + 1 \pmod 5$.

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?

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

(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?

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, where $k \leq d$, values?

p^{d+1-k} different polynomials. For $k = d+1$, there should only be 1 polynomial.

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 ≤ 2 such that $Q(0) \equiv w \pmod{59}$. Here are your x and $Q(x)$:

TA: write a unique $Q(x_i) = y_i$ here in every student's worksheet based on function $Q(x) = x^2 + x + 7 \bmod 59$: $Q(1) = 9, Q(2) = 13, Q(3) = 19, Q(4) = 27, Q(5) = 37, Q(6) = 49, Q(7) = 4, Q(8) = 20, Q(9) = 38, Q(10) = 58, Q(11) = 21, Q(12) = 45, Q(13) = 12, Q(14) = 40, Q(15) = 11, Q(16) = 43, Q(17) = 18, Q(18) = 54, Q(19) = 33, Q(20) = 14, Q(21) = 56, Q(22) = 41, Q(23) = 28, Q(24) = 17, Q(25) = 8, Q(26) = 1, Q(27) = 55, Q(28) = 52, Q(29) = 51, Q(30) = 52, Q(31) = 55, Q(32) = 1, Q(33) = 8, Q(34) = 17, Q(35) = 28, Q(36) = 41, Q(37) = 56, Q(38) = 14, Q(39) = 33, Q(40) = 54, Q(41) = 18, Q(42) = 43, Q(43) = 11, Q(44) = 40, Q(45) = 12, Q(46) = 45, Q(47) = 21, Q(48) = 58, Q(49) = 38, Q(50) = 20.$

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

3.

(b) Please find w.

Students should work in groups of 3 or more to find the number. $w = 7$.

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

TA: $P(1) = 6$. The polynomial will be $P(x) = x + 5 \bmod 11$ and thus $s = 5$.

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.

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

For the first condition: just one polynomial of degree at most $n-1$ 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 at most $m-1$ 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.

The previous set of two schemes remain the same. We just need polynomials for each country, so that only if the representatives of the country get together can the entire country help.

So, we have two more polynomials for each country, one for producing a point for each of the two schemes. These would be degree at most $k-1$ each, 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.