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

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 $\mathbb{R}$:

(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.

True. $-b/a$ is the sum of the two roots, while c/a is the product of the two roots. These must both be positive, while multiplying them through by the positive value a^2 shows they have the same signs as $-ab$ and ac, respectively.

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

The number of solutions of $P(x) = Q(x)$ is at most $\max(d_1, d_2)$. The number of solutions of $P(x) \cdot Q(x) = 0$ is at most $d_1 + d_2$. [We also know that, if d_1 and d_2 are both odd, then $P(x) \cdot Q(x)$ has at least one root, though this isn't terribly important]

(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?

If d is even, 0 (consider $x^d + 1$); otherwise, 1 (a polynomial of odd degree takes on arbitrarily large positive and negative values, and thus must pass through 0 inbetween them at least once).

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

If there is a root c, then the polynomial is divisible by $x - c$. Therefore it can be written as $(x - c)g(x)$. But $g(x)$ is a degree one polynomial and by looking at coefficients it is obvious that its leading coefficient is 1. Therefore $g(x) = x - d$ for some d. But then d is also a root, which means that $d = c$. So $f(x) = (x - c)^2$ which means that $a = -2c$ and $b = c^2$.

2. Roots: The Next Generations

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

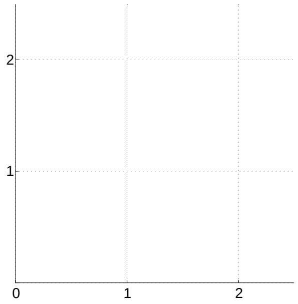
Which of the facts from above stay true when $\mathbb{R}$ is replaced by $GF(p)$ [i.e., integer arithmetic modulo the prime p]? Which change, and how? Which statements won't even make sense anymore?

It no longer makes sense to discuss positive vs. negative in the context of $GF(p)$, so 2a above becomes nonsense. The fact in 2d continues to hold in any field, as do the upper bounds on the number of roots in 2b and 2c. 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.

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 $(1, P(1))$.

TAs: Now, drawing on the board, expand the field (to, say, GF(7)). We now know that the points Alice wanted to send were $2, 1$. Encoding these over GF(7) we get the polynomial $P(x) = 6x + 2$. What if we didn't just have dropped packets, but had malicious errors? Start drawing in malicious errors so the students can see until when error-correction could work, how many points you would need to send, etc. Try to do this interactively.

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.
   Inverse pairs mod 5: $(1,1), (2,3), (4,4)$.

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

$$\begin{aligned}
\Delta_0 &= \frac{(x-3)(x-4)}{(0-3)(0-4)} = \frac{x^2-7x+12}{(-3)(-4)} = 3(x^2+3x+2) = 3x^2+4x+1 \\
\Delta_3 &= \frac{(x-0)(x-4)}{(3-0)(3-4)} = \frac{x^2-4x}{(3)(-1)} = 3(x^2+x) = 3x^2+3x \\
\Delta_4 &= \frac{(x-0)(x-3)}{(4-0)(4-3)} = \frac{x^2-3x}{(4)(1)} = 4(x^2+2x) = 4x^2+3x
\end{aligned}$$

Thus, our original polynomial P is

$$\begin{aligned}
4\Delta_0 + 1\Delta_3 + 2\Delta_4 &= 4(3x^2+4x+1)+(3x^2+3x)+2(4x^2+3x) \\
&= (2x^2+x+4)+(3x^2+3x)+(3x^2+x) \\
&= 3x^2+4
\end{aligned}$$

Linear equation way: Writing $P(x) = m_2x^2+m_1x+m_0$, we solve for the m_i's by solving the linear equation

$$\begin{bmatrix} 0 & 0 & 1 \\ 9 & 3 & 1 \\ 16 & 4 & 1 \end{bmatrix} \begin{bmatrix} m_2 \\ m_1 \\ m_0 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ 2 \end{bmatrix}$$

This gives the equation

$$\frac{1}{2}x^2 - \frac{5}{2}x + 4,$$

which, in the modulo 5 world, means $P(x) = 3x^2+4$.

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.

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

   For the first condition: just one polynomial of degree $\leq n-1$ or less 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 $m-1$ 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.

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.

(Hint: use $n+1$ polynomials.)

The previous set of two schemes remain the same. We just need polynomials for each country, so that the 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-$k-1$ 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.