DISCUSSION 07D

1 How Many Polynomials?

Let $P(x)$ be a polynomial of degree at most 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? 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 at most d over GF(p) are there if we only know k values, where $k \leq d$?

2 Proofs about Polynomials

In this problem, you will give two different proofs of the following theorem: For every prime p, every polynomial over GF(p) with degree $\geq p$ is equivalent to a polynomial of degree at most $p-1$. (Two polynomials f, g over GF(p) are said to be equivalent iff $f(x) = g(x)$ for all $x \in$ GF(p).)

(a) Show how the theorem follows from Fermat's Little Theorem.

(b) Now prove the theorem using properties of polynomials.

3 Properties of GF(p)

(a) Show that, if $p(x)$ and $q(x)$ are polynomials over the reals (or complex, or rationals) and $p(x) \cdot q(x) = 0$ for all x, then either $p(x) = 0$ for all x or $q(x) = 0$ for all x or both. (*Hint*: You may want to prove first this lemma, true in all fields: The roots of $p(x) \cdot q(x)$ is the union of the roots of $p(x)$ and $q(x)$.)

(b) Show that the claim in part (a) is false for finite fields GF(p).

4 Roots

Let's make sure you're comfortable with roots of polynomials in the familiar real numbers $\mathbb{R}$. Recall that a polynomial of degree d has at most d roots. In this problem, assume we are working with polynomials over $\mathbb{R}$.

(a) 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 $p(x) \cdot q(x) = 0$?

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

(c) What is the *minimum* number of real roots that a nonzero polynomial of degree d can have? How does the answer depend on d?

5 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?

6 Secret Sharing Practice

Consider the following secret sharing schemes and solve for asked variables.

(a) Warm-up: Create a scheme for 5 trick-or-treaters such that they can only open the bag of candy if 3 of them agree to open it.

(b) Let p be a degree 3 polynomial modulo 7, and $p(1) = 2, p(2) = 1, p(3) = 5, p(4) = 5$. Find p.

(c) Create a scheme for the following situation: There are 4 cats and 3 dogs in the neighborhood, and you want them to only be able to get the treats if the majority of the animals of each type are hungry.

7 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.

(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.