EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 6W

1. INTERPOL WARNING

Consider the set of four points $\{(-1,1),(0,2),(1,5),(2,40)\}$. Find the unique polynomial over $\mathbb{R}$ of degree ≤ 3 that passes through these points by solving a system of linear equations.

2. 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.

(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 $a^2 = 4b$.

3. 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 $\mathbf{GF}(p)$ [i.e., integer arithmetic modulo the prime p]? Which change, and how? Which statements won't even make sense anymore?