CS 70 Discrete Mathematics and Probability Theory
Summer 2017 Hongling Lu, Vrettos Moulos, and Allen Tang

DISCUSSION 08A

1 Polynomials in One Indeterminate

We will now prove a fundamental result about polynomials: every non-zero polynomial of degree n (over a field F) has at most n roots. If you don't know what a field is, you can assume in the following that $F = \mathbb{R}$ (the real numbers).

(a) Show that for any $\alpha \in F$, there exists some polynomial $Q(x)$ of degree $n-1$ and some $b \in F$ such that $P(x) = (x-\alpha)Q(x) + b$.

(b) Show that if α is a root of $P(x)$, then $P(x) = (x-\alpha)Q(x)$.

(c) Prove that any polynomial of degree 1 has at most one root. This is your base case.

(d) Now prove the inductive step: if every polynomial of degree $n-1$ has at most $n-1$ roots, then any polynomial of degree n has at most n roots.

2 Polynomial Short

(a) What is the minimum number of points necessary to uniquely determine a degree d polynomial?

(b) Let p be a degree 6 polynomial and q be a degree 4 polynomial. What is the maximum possible degree of $p+q$? What is the minimum possible degree? What about $p \cdot q$?

3 Polynomials in Fields

Define the sequence of polynomials by $P_0(x) = x+12$, $P_1(x) = x^2 - 5x + 5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$.

(For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.)

(a) Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in \mathbb{N}$.

(b) Show that, for every prime q, if $P_{2017}(x) \not\equiv 0 \pmod{q}$, then $P_{2017}(x)$ has at most 2017 roots modulo q.