CS 70 Discrete Mathematics and Probability Theory
Fall 2017 Satish Rao and Kannan Ramchandran

DIS 5B

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. Think of F as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or GF(p) for a prime p; your proofs should work equally well in each case.

(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, where n is an integer ≥ 2, then any polynomial of degree n has at most n roots.

2 Interpolate!

Find the lowest-degree polynomial $P(x)$ that passes through the points $(1,4),(2,3),(5,0)$ modulo 7.

3 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.