CS 70 Discrete Mathematics and Probability Theory DIS 3B Summer 2023 Huang, Suzani, and Tausik

Polynomial Practice 1

Note 8

- (a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)
 - (i) f + g
 - (ii) $f \cdot g$
 - (iii) f/g, assuming that f/g is a polynomial

- (b) Now let f and g be polynomials over GF(p).
 - (i) We say a polynomial f = 0 if $\forall x, f(x) = 0$. Show that if $f \cdot g = 0$, it is not always true that either f = 0 or g = 0.
 - (ii) How many f of degree exactly d < p are there such that f(0) = a for some fixed $a \in \{0, 1, \dots, p p\}$ 1?

(c) Find a polynomial f over GF(5) that satisfies f(0) = 1, f(2) = 2, f(4) = 0. How many such polynomials of degree at most 4 are there?

2 Interpolation Practice

Find the lowest degree polynomial with coefficients in \mathbb{R} that passes through the points (0,0), (1,2), and (2,-1). Now do it again in, with coefficients in GF(3).

3 Secrets in the United Nations

- A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.
 - (a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination *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: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. 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.