CS 70 Discrete Mathematics and Probability Theory
Fall 2019 Alistair Sinclair and Yun S. Song

DIS 5

1 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).

2 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.

3 Where Are My Packets?

Alix wants to send the message (a_0, a_1, a_2) to Bo, where each $a_i \in \{0,1,2,3,4\}$. She encodes this message using a polynomial f of degree ≤ 2 over GF(5) with the property that $f(0) = a_0$, $f(1) = a_1$, and $f(2) = a_2$, and she sends the packets $(0, f(0))$, $(1, f(1))$, $(2, f(2))$, $(3, f(3))$, $(4, f(4))$. Two packets are dropped, and Bob only learns that $f(0) = 4$, $f(3) = 1$, and $f(4) = 2$. Help Bo recover Alix's message!

(a) Find the multiplicative inverses of 1, 2, 3, and 4 modulo 5.

(b) Find the original polynomial f, either by using Lagrange interpolation or solving a system of linear equations.

(c) Recover Alix's original message.

4 Prime Polynomials

A polynomial $f(x)$ is called *prime* if it has degree at least 1 and it is not possible to write it as $f(x) = g(x)h(x)$, where g and h both have smaller degree than f. Prove that there are infinitely many prime polynomials with coefficients in GF(q). You may want to review the proof that there are infinitely many prime numbers, and it may in addition be helpful to prove that every polynomial is either prime or can be written as a product of prime polynomials.