1 Polynomial Practice

(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 $\text{GF}(p)$.

(i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. If $f \cdot g = 0$, is it 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 $a \in \{0, 1, \ldots, p - 1\}$?

(c) Find a polynomial $f$ over $\text{GF}(5)$ that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?
2 Rational Root Theorem

The rational root theorem states that for a polynomial

\[ P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \]

\[ a_0, \ldots, a_n \in \mathbb{Z}, \text{ if } a_0, a_n \neq 0, \] then for each rational solution \( \frac{p}{q} \) such that \( \gcd(p, q) = 1 \), \( p | a_0 \) and \( q | a_n \). Prove the rational root theorem.

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.
4  Old Secrets, New Secrets

In order to share a secret number $s$, Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree $n$ polynomial $p$ with her friends Bob$_1, \ldots, Bob_{n+1}$. As usual, she chose $p$ such that $p(0) = s$. Bob$_1$ through Bob$_{n+1}$ now gather to jointly discover the secret. Suppose that for some reason Bob$_1$ already knows $s$, and wants to play a joke on Bob$_2, \ldots, Bob_{n+1}$, making them believe that the secret is in fact some fixed $s' \neq s$. How could he achieve this? In other words, what value should he report in order to make the others believe that the secret is $s'$?