1 Polynomial Practice

Note 8

(a) If f and g are non-zero real polynomials, how many real 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 $a \in \{0, 1, \ldots, p-1\}$?

(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?

$4x^2 - 20x + 16 \equiv 4x^2 + 1$

2 Lagrange Interpolation in Finite Fields

Note 8

Find a unique polynomial $p(x)$ of degree at most 2 that passes through points $(-1,3)$, $(0,1)$, and $(1,2)$ in modulo 5 arithmetic using the Lagrange interpolation.

(a) Find $p_{-1}(x)$ where $p_{-1}(0) \equiv p_{-1}(1) \equiv 0 \pmod 5$ and $p_{-1}(-1) \equiv 1 \pmod 5$.

$p_{-1}(x) = k x(x-1)$ $\quad p_{-1}(-1) \equiv 2k \equiv 1 \pmod 5$ $\quad 2*3 - 5 = 1$

$[(-1-0)*(-1-1)]^{-1} = 2^{-1}$ $\quad k = 3$.

$p_{-1}(x) \equiv 3x(x-1) = 3x^2 - 3x$

(b) Find $p_0(x)$ where $p_0(-1) \equiv p_0(1) \equiv 0 \pmod 5$ and $p_0(0) \equiv 1 \pmod 5$.

$p_0(x) = k(x+1)(x-1)$ $\quad -k \equiv 1 \pmod 5$ $\quad k \equiv -1$

$p_0(x) \equiv -(x^2-1) \equiv 1 - x^2$ $\quad (x+1)(x-1)(-1)^{-1}$

(c) Find $p_1(x)$ where $p_1(-1) \equiv p_1(0) \equiv 0 \pmod 5$ and $p_1(1) \equiv 1 \pmod 5$.

$p_1(x) = k(x+1)x$ $\quad 2k \equiv 1 \pmod 5$ $\quad k = 3$

$p_1(x) \equiv 3x(x+1) = 3x^2 + 3x$

(d) Construct $p(x)$ using a linear combination of $p_{-1}(x)$, $p_0(x)$, and $p_1(x)$.

$p(x) \equiv 3p_{-1}(x) + p_0(x) + 2p_1(x)$

$\equiv 3(3x^2 - 3x) + 1 - x^2 + 2(3x^2 + 3x)$

$\equiv (4x^2 - 3x + 1) \equiv 4x^2 - 3x + 1$

3 Secrets in the United Nations

Note 8

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.

choose a prime $p > 193$ work on $GF(p)$ $p > 193 + 138$

$p(x)$ of degree 192

$p(0) =$ secret $\quad p(1) \ldots p(193)$ give to 193 member countries.

138 $p(194) \ldots p(332)$ gives to Secretary-General

(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.

for p(1) to p(193)

q(x) of degree (11) ... work on GF(p)

let p(0) = q(0) → give q(1), q(2) ... q(12) to

12 representatives

4 To The Moon!

Note 8

A secret number s is required to launch a rocket, and Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree n polynomial p to a group of \$GME holders $\text{Bob}_1, \ldots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. However, Bob_1 is secretly a partner at Melvin Capital and already knows s, and wants to sabotage $\text{Bob}_2, \ldots, \text{Bob}_{n+1}$, 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 terms variables known in the problem, such as s', s or y_1) in order to make the others believe that the secret is s'?

$p(x) = a_n x^n + a_{n-1} x^{n-1} - 1 \ \ldots + s$

X

$p(1) = a_n + a_{n-1} + \ldots + a_1 + s$

$p(1) - s + s'$

$s = y_1 \Delta_1(0) + \sum_{k=2}^{n+1} y_k \Delta_k(0)$

$s' = y_1' \Delta_1(0) + \sum_{k=2}^{n+1} y_k \Delta_k(0)$

$s - s' = \Delta_1(0)(y_1 - y_1')$

$y_1' = (\Delta_1(0))^{-1}(s' - s) + y_1$

$\Delta_1(x)$ root $2 - n+1 \to n$ root

↓ degree, n

so $\Delta_1(0) \neq 0$.