Polynomials:

- nonzero polynomial of degree d has at most d roots
- A unique polynomial of degree $\leq d$ passes through any $d+1$ points
- $GF(p)$ means we are working under mod p for prime p

ex. in $GF(3)$, $f(x) = 2x + 2$ has root $x = 2$

$f(2) = 2(2) + 2 = 6 \equiv 0 \pmod 3$

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

(i)

- could have 0 roots: $f(x) = 2x^2 - 1$, $g(x) = -x^2 + 2$

  $f(x) + g(x) = x^2 + 1$

- $f+g$ has at most $\max(\deg f, \deg g)$ roots

(ii)

- could have 0 roots: $f(x) = g(x) = x^2 + 1$
- $f \cdot g$ has at most $\deg f + \deg g$ roots b/c

if $f(x)g(x) = 0$ for some x, x is a root of f or g

(iii)

- could have 0 roots: $f(x) = g(x)(x^2+1)$

  $(f/g)(x) = x^2 + 1$

- f/g is a polynomial $\Rightarrow$ f/g has degree $\deg f - \deg g$

so there are at most $\deg f - \deg g$ roots

(b) Now let f and g be polynomials over GF(p), where p is prime.

(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 $a \in \{0, 1, \ldots, p-1\}$?

(i) No. In GF(2) let $f(x) = 1 - x$

$g(x) = x$

$f(0) = 1, \ f(1) = 0$

$g(0) = 0, \ g(1) = 1$

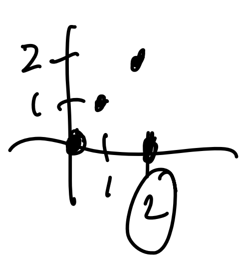
$(p+1)x \equiv x \pmod p$

$px + x$

(ii) $f(x) = c_d \cdot x^d + c_{d-1} \cdot x^{d-1} + \ldots + c_0$

- in general, each of $d+1$ coefficients of f can take on p values
- constant coefficient $f(0) = c_0 = a$ is fixed, also top coefficient c_d can't be 0
- $p-1$ possible values for c_d, p possible values for $d-1$ coefficients

$\boxed{(p-1)p^{d-1}}$



(x_i, y_i)

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

- polynomial over GF(p) can be degree at most 4 which is determined by 5 points. 3 points are given to us, leaving $5 \cdot 5 = 25$ possible polynomials.

By Lagrange Interpolation: $f(x) = \Delta_0(x) + 2\Delta_2(x) + 0 \cdot \Delta_4(x)$

$$\boxed{\Delta_i(x) = \begin{cases} 1 & \text{if } x = i \\ 0 & \text{if } x \neq i \end{cases}}$$

$$\Delta_0(x) = \frac{(x-2)(x-4)}{(0-2)(0-4)} = \frac{1}{8}(x-2)(x-4)$$

$$\equiv (3^{-1} \bmod 5)(x-2)(x-4) \pmod 5$$

$$\equiv 2(x-2)(x-4) \pmod 5$$

$$\Delta_2(x) = \frac{x(x-4)}{2(2-4)} = -\frac{1}{4}x(x-4)$$

$$\equiv x(x-4) \pmod 5$$

$$f(x) = 2(x-2)(x-4) + 2x(x-4)$$

$$= 2(x-4)[x-2+x]$$

$$= 2(x-4)(2x-2)$$

$$= 2(2x^2 - 10x + 8)$$

$$\equiv 4x^2 + 1 \qquad (\text{mod } 5)$$

2 Rational Root Theorem

The rational root theorem states that for a polynomial

i.e. root of P

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

$a_0, \cdots, a_n \in \mathbb{Z}$, 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.

if $\frac{p}{q}$ is a root of P:

$$P\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

multiply by q^n on both sides:

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0$$

$p | a_0$:

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} = -a_0 q^n$$

$$p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \ldots + a_1 q^{n-1}) = -a_0 q^n$$

so $p | a_0 q^n \Rightarrow p | a_0$ since p, q coprime

$q | a_n$:

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0$$

$$a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = -a_n p^n$$

$$q(a_{n-1} p^{n-1} + \ldots + a_1 p q^{n-2} + a_0 q^{n-1}) = -a_n p^n$$

so $q | a_n p^n \Rightarrow q | a_n$ since p, q coprime

Secret Sharing: n total officials, want a scheme so that any group of k officials can pool their info together to figure out secret

- make a deg $k-1$ polynomial, give a point (i, y_i) to the ith official
- work under $GF(p)$ where $p > k$

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.

create a degree 192 polynomial. Give each country 1 point, give the Secretary-General $193 - 55 = 138$ points. $193 + 138$ pts. in total

(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.

Add onto scheme from part a):

For every country, construct a degree 11 polynomial f_i & give each of 12 representatives one point. Make $f_i(0) = t_i$ where t_i is the country's point on the degree 192 polynomial.