1. Polynomial Definition
   - ↳ Property 1
   - ↳ Property 2
2. Polynomial Interpolation
3. Property 2 Proof
4. Polynomial Division
5. Property 1 Proof.
6. Finite Fields
7. Counting
8. Secret Sharing

---

9. CRT vs Lagrange Comparison

HW2 Q1 was updated w/ Gradescope Quiz

Polynomial Definition

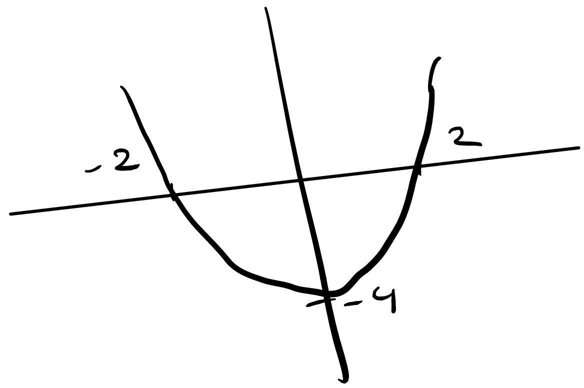
$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

x is a variable

a_i are coefficients

The degree d is the exponent of the highest order term

Ex: $p(x) = x^2 - 4$



Property 1

Property 2

Polynomial Interpolation

Given $d+1$ pairs $(x_1, y_1) \ldots (x_{d+1}, y_{d+1})$, what <u>is</u> the unique degree (at most) d polynomial that goes through those points?

Polynomial Interpolation Example

$(x_1, y_1) = (1, 1)$

$(x_2, y_2) = (2, 2)$

$(x_3, y_3) = (3, 4)$.

Property 2 Proof

Property 2

Given $d+1$ pairs $(x_1, y_1) \ldots (x_{d+1}, y_{d+1})$, with all x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \le i \le d+1$

Proof:

Polynomial Division

$p(x)$ polynomial of degree d

Can divide $p(x)$ by polynomial $q(x)$

of degree $\leq d$ using long division

$$p(x) = q'(x) \cdot q(x) + r(x)$$

quotient

remainder (deg. $r(x)$ is less than deg $q(x)$)

Example:

Proof of Property 1

Property 1

A nonzero polynomial of degree d has at most d roots

Proof:

Claim 1: If a is a root of a polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x-a)\,q(x)$ for a polynomial $q(x)$ with degree $d-1$

Claim 2: A polynomial $p(x)$ of degree d with distinct roots $a_1, \ldots, a_d$ can be written as $p(x) = c\,(x-a_1)\cdots(x-a_d)$ where c is a real number. $(c \neq 0)$

Note: Claim 2 $\Rightarrow$ Property 1

Also, $p(x)$ cannot have some other root $a \neq a_i$ $i = 1, \ldots, d$ since $p(a) = c(a-a_1)\cdots(a-a_d) \neq 0$

Proof of Claim 1

Proof of Claim 2

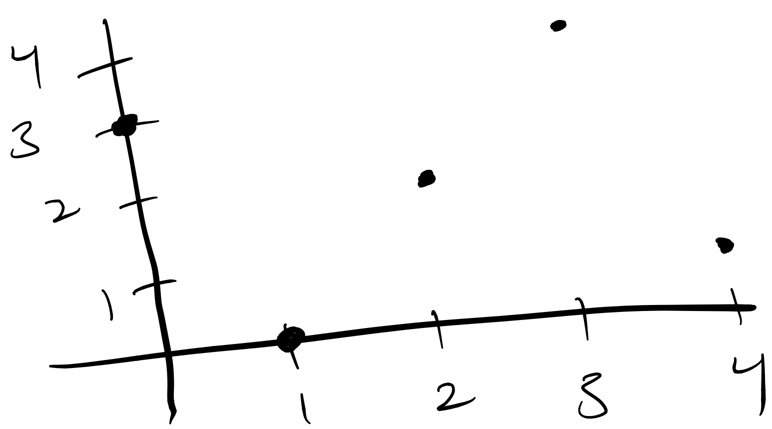
Finite Fields

So far, we just used $+, -, \times, \div$

If m is prime, then these operations still work mod m

coefficient must be values mod m
variables must be values mod m

Consider $p(x) = 2x + 3 \pmod 5$



Working mod m where m is prime
"working in a finite field"
GF (m) "Galois Field"

Note: No fractions when working mod m, use multiplicative inverses!

Counting

How many degree d polynomials are there when working mod m?

Secret Sharing

Share nuclear launch codes such that

(1) Any subset of k officials can compute code and launch together

(2) No group of $k-1$ or fewer have any info about the code if they pool their info together.