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

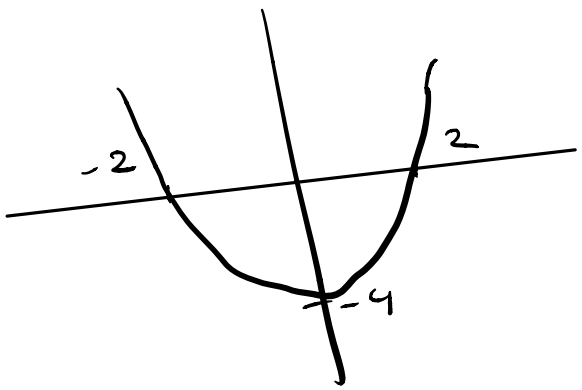
$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$$

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

A nonzero polynomial of degree d has at most d roots.

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 $1 \leq i \leq d+1$

Polynomial Interpolation

Given $d+1$ pairs $(x_1, y_1) \dots (x_{d+1}, y_{d+1})$, what is the unique degree (atmost) d polynomial that goes through those points?

Consider $p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$

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

"delta polynomial"
"switch"
"basis vector"

This works since only one $\Delta_i(x)$ is "on" for a given x_i input, and outputs its y_i

$$\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}$$

This procedure is called Lagrange Interpolation.

Polynomial Interpolation Example

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

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

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

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{1}{2}x^2 - \frac{5}{2}x + 3$$

$$\Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = -x^2 + 4x - 3$$

$$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = \frac{1}{2}x^2 - \frac{3}{2}x + 1$$

$$p(x) = 1 \cdot \Delta_1(x) + 2\,\Delta_2(x) + 4\,\Delta_3(x)$$

when $x = x_1$,

$$1 \cdot 1 + 2 \cdot 0 + 4 \cdot 0 = 1$$

$p(x_1) = 1$

$$p(x) = \frac{1}{2}x^2 - \frac{1}{2}x + 1$$

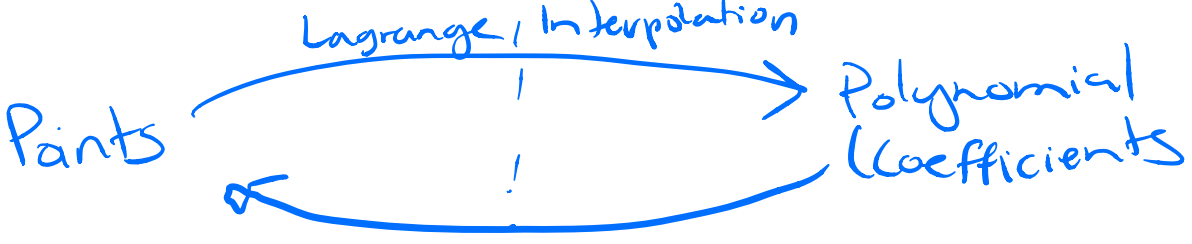
Property 2 Proof

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 $1 \leq i \leq d+1$

Proof: Must show $p(x)$ exists and is unique

Existence: Can use Lagrange Interpolation



(x_1, y_1)

$\vdots$

(x_{d+1}, y_{d+1})

$a_d x^d + \ldots + a_1 x + a_0$

Easy to evaluate at new points.

$p(x_i) \cdot q(x_i)$

Easy to multiply polynomials at known points.

Uniqueness

Assume toward contradiction that there is another

polynomial $q(x)$ such that $q(x_i) = y_i$ for all $d+1$ pairs.

Consider $r(x) = p(x) - q(x)$

↗ ↳ $r(x)$ is degree at most d

↳ $r(x)$ has $d+1$ roots

Contradicts Property 1 (to be proved)

$\Rightarrow$ $p(x)$ is unique.

Polynomial Division

$p(x)$ polynomial of degree d

Can divide $p(x)$ by polynomial $q(x)$ of degree $\leq d$ using long division

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

$q'(x)$: quotient

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

Example:

$p(x) = x^3 + x^2 - 1$

$q(x) = x - 1$

$$\begin{array}{r} x^2 + 2x + 2 \\ x-1 \;\overline{)\; x^3 + x^2 - 1} \\ x^3 - x^2 \\ \hline 2x^2 - 1 \\ 2x^2 - 2x \\ \hline 2x - 1 \\ -\;\; 2x - 2 \\ \hline 1 \end{array}$$

$\Rightarrow q'(x) = x^2 + 2x + 2 \quad r(x) = 1$

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

$\rightarrow p(x) = (x-a)\,q(x) + r(x)$

must be degree 0 $\rightarrow$ some constant c

$p(a) = 0$ since a is a root

$= (a-a)\,q(a) + c$

$\Rightarrow c = 0 \rightarrow p(x) = (x-a)\,q(x)$

Proof of Claim 2

Proceed by induction on degree d

Base Case: $d = 0$

$p(x)$ is a constant c ✓

Inductive Hypothesis: For $d \geq 0$, any degree d polynomial can be written as $p(x) = c(x-a_1)\cdots(x-a_d)$

Inductive Step:

Let $p(x)$ be a polynomial of deg $d+1$ w/ distinct roots $a_1, \ldots, a_{d+1}$

By Claim 1,

$$p(x) = \underbrace{(x - a_{d+1})}\, q(x)$$

Nonzero when you plug in $a_1, \ldots, a_d$ ⇒ must be zero when plugging in $a_1, \ldots, a_d$

Since $a_i \neq a_j$ for $i \neq j$

So, we can apply the I.H. to $q(x)$

$q(x) = c(x-a_1)\cdots(x-a_d)$

$\Rightarrow p(x) = (x-a_{d+1})\left(c(x-a_1)\cdots(x-a_d)\right)$ ✓

Finite Fields

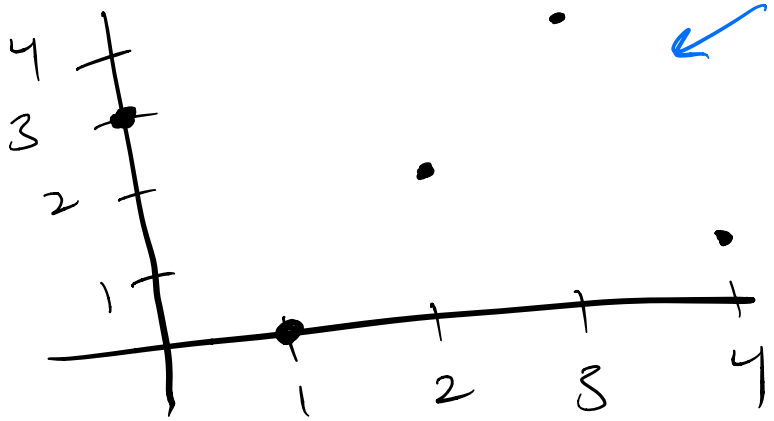
So far, we just used $+, -, \times, \div$

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

coefficient must be values mod m

variable 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 (at most degree d) polynomials are there when working mod m?

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x_1 + a$$

m choices for each coeff. $\Rightarrow m^{d+1}$

$(x_1, \quad)$

$(x_2, \quad)$

$\vdots$

$(x_{d+1}, \quad)$

m choices for each y value.

$\Rightarrow m^{d+1}$ polynomials when working mod m (m prime)

Secret Sharing

s is the secret.

Share nuclear launch code (s) 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.

k = 3

Secret Sharing Scheme (working mod m, m is prime)

1.) Pick a random polynomial $p(x)$ of degree $k-1$ such that $p(0) = s$

2.) Give $p(1)$ to the first official,
$p(2)$ to the second official
⋮

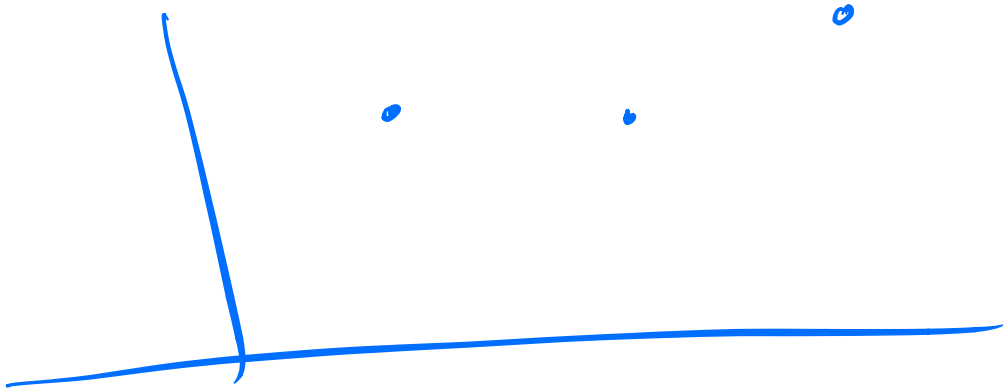
Observe: (1) Any k officials can use Lagrange Interpolation to compute $p(x)$ eval at $x=0$ to get s.

(2) Any group of k-1 or fewer

about s.

officials have no info

k-1 ppl.



at least m options for missing piece

m possible poly. of deg. k-1 going through these k-1 points.

There are m options for S.