

CS70 – SPRING 2026

LECTURE 10: FEB. 19

New Topic: Polynomials

- Basic properties of polynomials
 - Polynomials mod p
 - Application I: Secret Sharing
 - Application II: Error-Correcting Codes
- } TODAY
- } NEXT LEC.

Polynomials (over the real numbers)

Defn: A polynomial in a single variable x is a function of the form

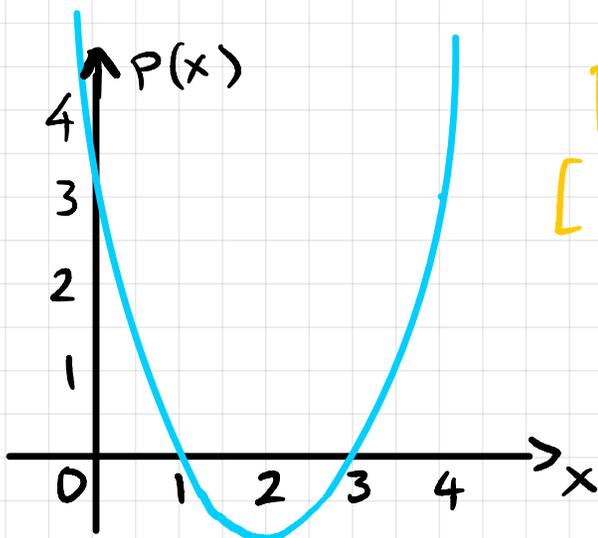
$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

degree d

coefficients a_i (real)

Examples: $p(x) = 7x + 3$ (degree 1)

$$p(x) = x^2 - 4x + 3 \quad (\text{degree } 2)$$
$$[= (x-3)(x-1)]$$

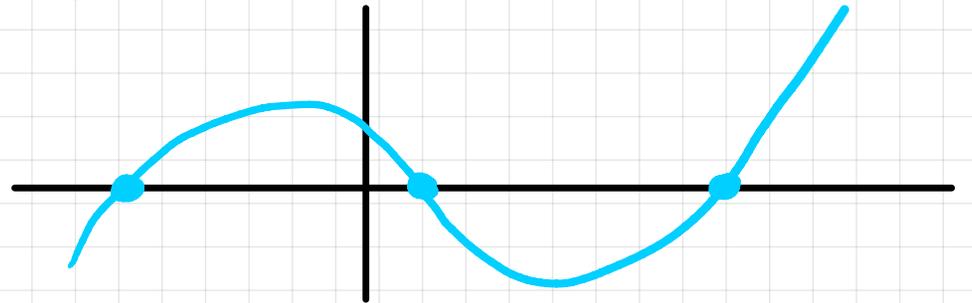


Defn: a is a root of $p(x)$ if $p(a) = 0$

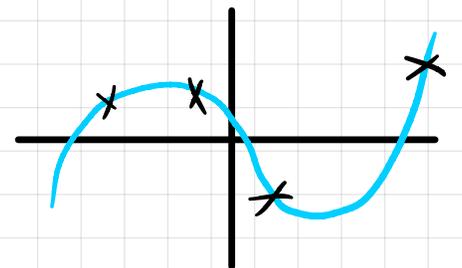
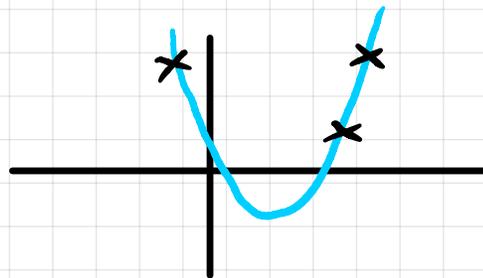
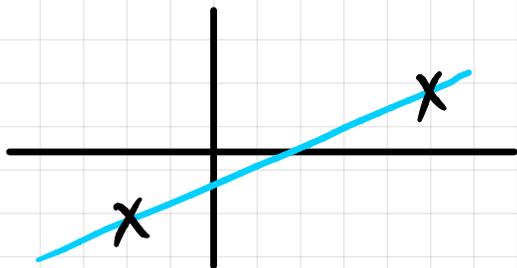
Polynomials: 2 Key Properties

Property 1: A non-zero polynomial of degree d has at most d roots

Eg. $d=3$ (cubic)



Property 2: Given $d+1$ pairs $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$, with all the x_i distinct, there exists a unique polynomial of degree $\leq d$ s.t. $p(x_i) = y_i$ for $1 \leq i \leq d+1$



Property 1: A non-zero polynomial of degree d has at most d roots

Proof: Let a_1, \dots, a_d be distinct roots of p . We (sketch) show p can be written as

$$p(x) = c(x-a_1)(x-a_2)\dots(x-a_d) \quad (*)$$

for some constant c .

Assuming $(*)$, if $a \neq a_1, \dots, a_d$ then

$$p(a) = c(a-a_1)(a-a_2)\dots(a-a_d) \neq 0$$

So no other a is a root! \square

Proof of $(*)$: see Notes (induction on d)

Property 2: Given $d+1$ pairs $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$, with all the x_i distinct, there exists a unique polynomial of degree $\leq d$ s.t.
 $p(x_i) = y_i$ for $1 \leq i \leq d+1$

Proof: We give an algorithm, called "Lagrange Interpolation", to construct $p(x)$
degree d

Method: Suppose we can construct "basis" polynomials $\Delta_i(x)$ for $1 \leq i \leq d+1$ s.t.

$$\Delta_i(x) = \begin{cases} 1 & \text{if } x = x_i \\ 0 & \text{if } x = x_j, j \neq i \end{cases}$$

Then we set $p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$ ✓

~~$p(x_i) = y_1 \Delta_1(x_i) + y_2 \Delta_2(x_i) + \dots + y_i \Delta_i(x_i) + \dots + y_{d+1} \Delta_{d+1}(x_i)$~~

Suppose we can construct "basis" polynomials $\Delta_i(x)$ for $1 \leq i \leq d+1$ s.t.

$$\Delta_i(x) = \begin{cases} 1 & \text{if } x = x_i \\ 0 & \text{if } x = x_j, j \neq i \end{cases}$$

Let $q_i(x) = (x-x_1)(x-x_2)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_{d+1})$

Then: • degree of q_i is d

• $q_i(x_j) = 0 \quad \forall j \neq i$

• $q_i(x_i) = \prod_{j \neq i} (x_i - x_j) \neq 0$

← OMIT $(x-x_i)$

So we can define

$$\Delta_i(x) = \frac{q_i(x)}{q_i(x_i)}$$

$$= \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_{d+1})}{(x_i-x_1)(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_{d+1})}$$

Example: Find degree-2 polynomial through $(0, -1)$, $(2, 2)$, $(3, 4)$

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(0-2)(0-3)} = \frac{1}{6}(x-2)(x-3)$$

$$\Delta_2(x) = \frac{(x-0)(x-3)}{(2-0)(2-3)} = -\frac{1}{2}x(x-3)$$

$$\Delta_3(x) = \frac{(x-0)(x-2)}{(3-0)(3-2)} = \frac{1}{3}x(x-2)$$

$$p(x) = -1 \times \Delta_1(x) + 2 \times \Delta_2(x) + 4 \times \Delta_3(x)$$

$$= -\frac{1}{6}(x-2)(x-3) - x(x-3) + \frac{4}{3}x(x-2)$$

$$= \dots$$

$$= \frac{1}{6}x^2 + \frac{7}{6}x - 1$$

Proof that $p(x)$ is unique:

Suppose for ~~\exists~~ \exists two different polynomials $p_1(x), p_2(x)$ of degree $\leq d$ that both go through the $d+1$ points $(x_1, y_1) \dots (x_{d+1}, y_{d+1})$

Then $q(x) := p_1(x) - p_2(x)$ is a non-zero poly. of degree $\leq d$.

But $q(x_i) = p_1(x_i) - p_2(x_i) = 0$ for x_1, x_2, \dots, x_{d+1}

So q is a poly. of degree $\leq d$ with $d+1$ roots! ~~\exists~~ Prop. 1

This concludes proof of Property 2. \square

Polynomials + Modular Arithmetic

Let p be prime

Integers mod p "behave like" real numbers, in that they support:

- 0 & 1 $[x+0=x; x*0=0; x*1=x]$
- operations of addition, subtraction, multiplication, division (inverses)

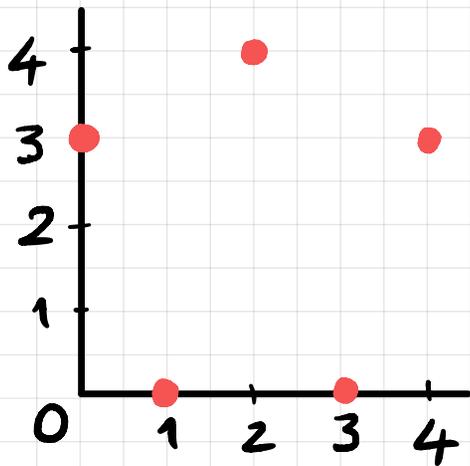
Technically, integers mod p are a field

Denote this field \mathbb{Z}_p or $\mathbb{GF}[p]$

Unlike $\mathbb{R}, \mathbb{Q}, \mathbb{C}$, $\mathbb{GF}[p]$ is a finite field

Polynomials over $GF[p]$

Example: $p(x) = x^2 - 4x + 3 \pmod{5}$



$$p(0) = 3$$

$$p(1) = 0$$

$$p(2) = 4$$

$$p(3) = 0$$

$$p(4) = 3$$

Key Fact: Polynomials over $GF[p]$ "behave like" real polynomials, in that they satisfy Properties 1 & 2 !

We can use Property 2 to count polynomials over $GF[p]$

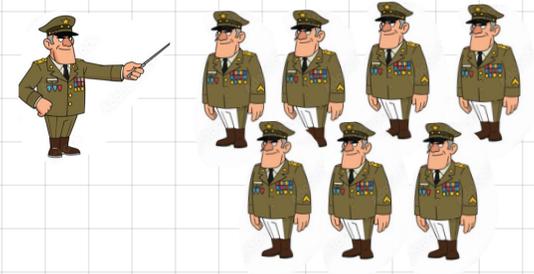
Q: How many different polys of degree $\leq d$ are there (mod p) ?

A: $p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$
 $\rightarrow p^{d+1} \quad (0, y_0) \quad (1, y_1) \quad \dots \quad (d, y_d)$

Q: Suppose I give you $k \leq d+1$ points. How many such polys. go through those points ?

A: p^{d+1-k}

Application: Secret Sharing



Commander wants to share a secret code s among n generals s.t.

- any group of $\geq k$ generals can figure out s
- any group of $< k$ generals has no information about s

Method

- Commander constructs a random polynomial $p(x)$ of degree $k-1$ (mod p)^{*} s.t. $p(0) = s$
- Commander gives each general i the value $p(i)$ ($i = 1, 2, \dots, n$)

* Need to choose $p > s$
Eg. $p = 1,000,003$
for 6-digit codes

- Commander constructs a random polynomial $p(x)$ of degree $k-1 \pmod{p}$ s.t. $p(0) = s$
 - Commander gives each general i the value $p(i)$ ($i=1, 2, \dots, n$)
-

Why does this work?

(i) Sp. k generals get together

They have k points on a degree- $(k-1)$ poly.
→ can use Lagrange to find $p(x)$
→ can evaluate $p(0) = s$

(ii) Sp. only $k-1$ (or fewer) generals get together

They have at most $k-1$ points on deg- $(k-1)$ poly.
→ still p possibilities for secret $p(0)$

Example: $n = 7$ generals | $p = 11$ | Polynomial
 $k = 3$ | $s = 8$ | $p(x) = x^2 + 6x + 8$

Suppose generals 1, 2, 7 get together

They have points $(1, 4), (2, 2), (7, 0)$

Lagrange:

$$\Delta_1(x) = \frac{(x-2)(x-7)}{(1-2)(1-7)} = 6^{-1}(x-2)(x-7) \equiv 2(x-2)(x-7) \pmod{11}$$

$[x_1 = 1]$

$$\Delta_2(x) = \frac{(x-1)(x-7)}{(2-1)(2-7)} = -5^{-1}(x-1)(x-7) \equiv 2(x-1)(x-7) \pmod{11}$$

$[x_2 = 2]$

$$\Delta_3(x) = \langle \text{whatever} \rangle$$

$[x_3 = 7]$

Note: All arithmetic must be done mod 11
So, e.g., $6^{-1} = 2 \pmod{11}$

Hence $p(x) = 4 \cdot \Delta_1(x) + 2 \cdot \Delta_2(x) + 0 \cdot \Delta_3(x)$

$$= 8(x-2)(x-7) + 4(x-1)(x-7) = \dots \equiv x^2 + 6x + 8 \pmod{11}$$

Secret sharing works the same way over \mathbb{R} .
Why do we do it over $GF[p]$?

- Keeps all arithmetic exact and numbers moderate sized integers. (Note : even over \mathbb{R} , we would choose integer coeffs. for $p(x)$)
- Can precisely quantify how much info. any subset of generals have
- With real polynomials, smaller group of generals can use the fact that coefficients are integers to learn something about the secret s (see next slide for example)

for integer coeffs. a, b, c

Example: Sp. $p(x) = ax^2 + bx + c$ / and 2 generals have the points $(1, 0)$ and $(2, 6)$.

Then they know:

$$\left. \begin{array}{l} p(1) = a + b + c = 0 \\ p(2) = 4a + 2b + c = 6 \end{array} \right\} \begin{array}{l} \text{solve for } b, c \text{ in terms} \\ \text{of } a : \\ b = 6 - 3a \\ c = 2a - 6 \end{array}$$

$$\text{So } p(x) = ax^2 + (6 - 3a)x + (2a - 6)$$

And a must be an integer

So the secret $s = p(0) = 2a - 6$ is even!

[With bigger values (x_i, y_i) for the points, we can learn even more about the secret!]