Lecture 3B: Polynomials, Secret Sharing

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- **HW 3** and **Vitamin 3** have been released, due **Thursday** (grace period Fri)
- HW 3 covers last Wednesday, Thursday and Yesterday's lecture.
- In this lecture, we will use small prime numbers as examples but in implementation we use large prime numbers (256 bits $\approx 10^{77}$ or more).

Finite Fields

Recall, that we talked about mod as a space.

When operating in a mod p where p is prime, we are working in a **finite field**.
A finite field is just a space of numbers, where we can define addition, subtraction, multiplication and division for all numbers in that space.

math 113/114

We will call this finite field a "Galois Field," denoted $GF(p)$

mod p

$GF(p)$

Polynomials in GF(p)

A **polynomial** in GF(p)

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

is specified by **coefficients** $a_d, \ldots, a_0$

$f(x)$ **contains** point (a, b) if $b = f(a)$

Polynomials over reals: $a_d, \ldots, a_0 \in \Re$, use $x \in \Re$

Polynomials in GF(p) have $a_d, \ldots, a_0 \in \{0, \ldots, p\text{-}1\}$, use $x \in \{0, \ldots, \text{p-1}\}$

Example: $f(x) = 2x^3 - 2x$ $= 2x^3 + 0x^2 + (-2)x + 0$

$a_3 = 2$

$a_2 = 0$

$a_1 = -2$

$a_0 = 0$

$f(2) = 2(2)^3 - 2(2)$

$= 2 \cdot 8 - 4$

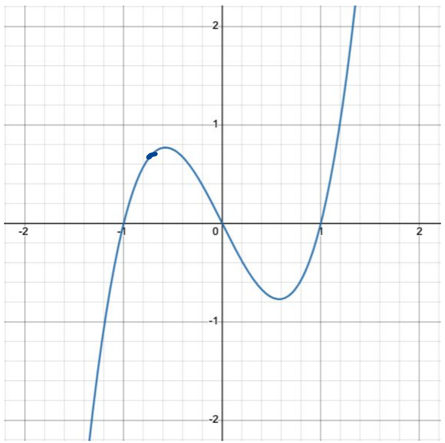
$= 2$

Contains?

$(1, 2)$? No $f(1) \neq 2$

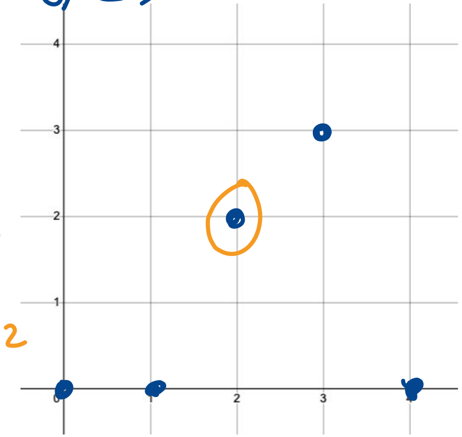
$(2, 2)$? Yes

Reals



GF(5)

f(x)



Polynomials in GF(p)

A **polynomial** in GF(p) degree

$x^0 = 1$

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

is specified by **coefficients** $a_d, \ldots, a_0$

$f(x)$ **contains** point (a, b) if $b = f(a)$

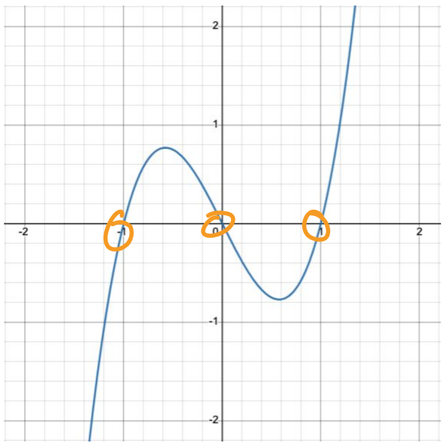
The **degree** of a polynomial is the highest exponent in the polynomial

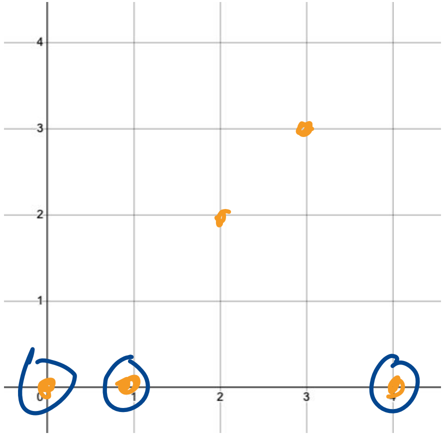
We say that a is a **root** (or **zero**) of a polynomial if $f(a) = 0$

degree

Example: $f(x) = 2x^3 - 2x$

$2x^3 - 2x$





Degree $d \Rightarrow$ at most d roots

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

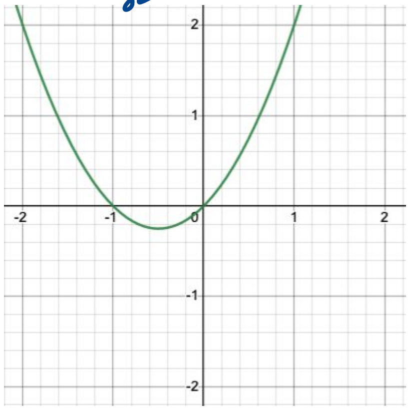
FLT $a^{p-1} \equiv 1 \mod p$

$a \in \{1, \ldots, p-1\}$

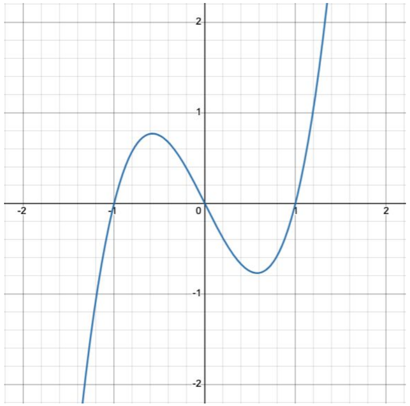
$GF(5)$

Examples:

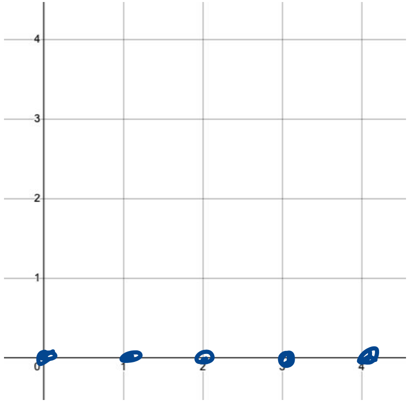
$x^2 + x$



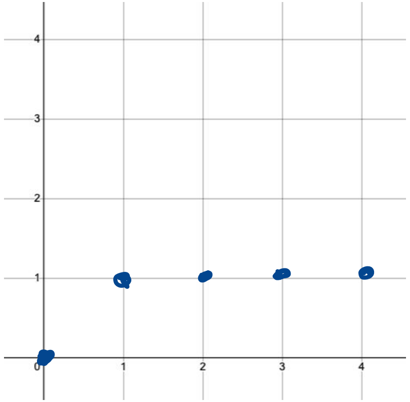
$2x^3 - 2x$

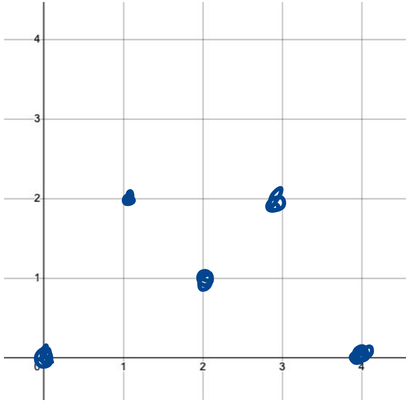


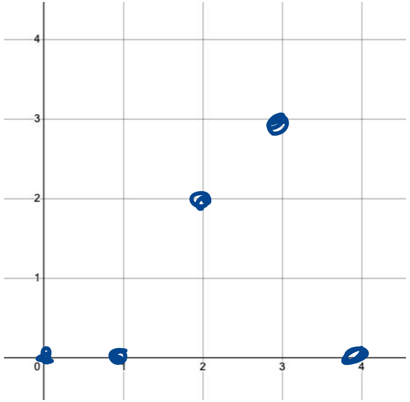
$f(x) = 0$



$f(x) = x^4$







d+1 points ⇒ unique degree d polynomial

We say a **point** is a x, y pair where $y = f(x)$

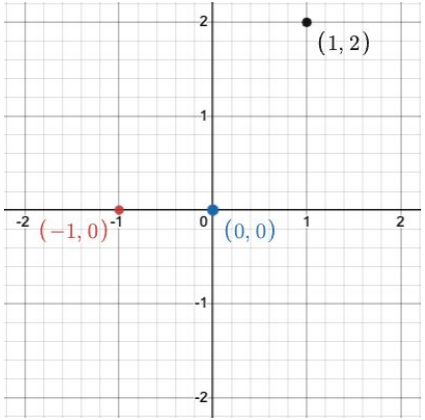
<u>Property 2:</u>
Given d+1 pairs: $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with all the x_i distinct, there is a unique polynomial $f(x)$ of degree (at most) d such that $f(x_i) = y_i$ for $1 \le i \le d+1$

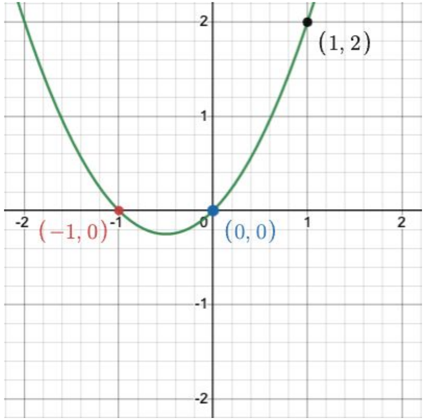
[There is a unique degree d polynomial that goes through a given set of d+1 points] Key idea

Example:

Given 3 points → Degree 2 polynomial

Points
$(-1, 0)$
$(0, 0)$
$(1, 2)$
→ $x^2 + x$





Implication of Properties on a Line

Slope

y-intercept

$\Rightarrow y = mx + b$

Suppose we have some linear polynomial

$$f(x) = a_1x + a_0$$

Property 1 says that if the line isn't just $f(x) = 0$ (x-axis) then it has at most 1 root.
Property 2 says two points define a line.

How to find a line that goes through a given two points:
Example: (1, 2) and (3, 4)

$y = mx + b$

$m = \frac{4-2}{3-1} = \frac{2}{2} = 1$

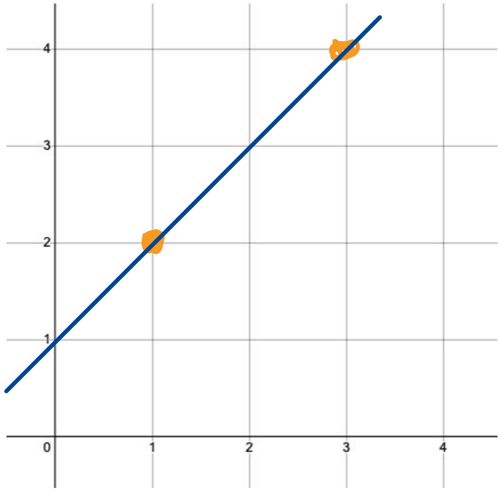
y-intercept

$2 = (1)(1) + b$

$2 = 1 + b$

$b = 1$

$f(x) = 1 \cdot x + 1$



Polynomial Equivalence

$a^{p-1} \equiv 1 \pmod{p}$

We state that two polynomials *f* and *g* are equivalent if for all *x* in *GF*(*p*), *f*(*x*) = *g*(*x*)

You can also show two polynomials are equivalent if they have the exact same coefficients.

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

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

Examples in *GF*(7):

$f_1(x) = x + 1$

$f_2(x) = 8x + 1$ $\quad 8 \equiv 1 \pmod{7}$

$f_3(x) = x + 8$ $\quad 8 \equiv 1 \pmod{7}$

$f_4(x) = x^7 + 1$

by FLT ✓

$\underbrace{x^6}_{1} \cdot x + 1$

$x + 1$

$f_1(0) = 1$

$f_4(0) = 1$ ✓

Polynomials from Points via Interpolation

Find the degree two polynomial in $\underbrace{GF(5)}_{}$ that contains $(1, 2)$; $(2, 4)$; $(3, 0)$

mod 5

$y_1 \quad y_2 \quad y_3$

$p(x) = y_1 \cdot \Delta_1(x) + y_2 \cdot \Delta_2 x + y_3 \cdot \Delta_3(x)$

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

$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = 3(x-2)(x-3) = 3x^2 - 15x + 18 = 3x^2 + 3$

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

$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = 3(x-1)(x-2) = 3x^2 - 9x + 6 = 3x^2 + x + 1$

$p(x) = 2(3x^2 + 3) + 4(4x^2 + 4x + 2) + 0(3x^2 + x + 1)$

$= 2x^2 + x + 4$

p(x) contains these points

x	$2x^2 + x + 4$
1	$2(1)^2 + 1 + 4 \equiv 7 \equiv 2$ ✓
2	$2(2)^2 + 2 + 4 \equiv 4$ ✓
3	$2(3)^2 + 3 + 4 \equiv 0$ ✓

Polynomials from Points via Gaussian Elimination

Find the degree two polynomial in $GF(5)$ that contains (1, 2); (2, 4); (3, 0)

$f(x) = a_2x^2 + a_1x + a_0$

input	
1	$2 = a_2(1)^2 + a_1(1) + a_0$
2	$4 = a_2(2)^2 + a_1(2) + a_0$
3	$0 = a_2(3)^2 + a_1(3) + a_0$

$$2 = a_2 + a_1 + a_0$$
$$4 = 4a_2 + 2a_1 + a_0$$
$$0 = 9a_2 + 3a_1 + a_0$$

Why you need d+1 points for degree d

d+1 unknown coefficients

Proving Property 2

Property 2: Given d+1 pairs: $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with all the x_i distinct, there is a unique polynomial $f(x)$ of degree (at most) d such that $f(x_i) = y_i$ for $1 \le i \le d+1$
"d+1 points, define a unique degree d polynomial"

?

1. We showed the existence of a polynomial via interpolation
2. We need to show uniqueness

Proof for uniqueness:

Assume for contradiction that given some $d+1$ points there exist two degree d polynomials that contain the same $d+1$ points, call them $p(x)$ and $q(x)$. Since, $p(x) \neq q(x)$
* $p(x) - q(x) \neq 0$. Notice that $p(x) - q(x)$ is then a degree d polynomial at most. But $p(x) - q(x) = 0$ for the $d+1$ points that p and q share. This is a contradiction since by Property 1 $p(x) - q(x)$ can have d roots at most.

* $p(x) - q(x) \neq 0$ means it's not always zero.

Long Division

It is possible to divide polynomials. That is dividing $p(x)$ by $q(x)$ results in

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

quotient remainder

$$\frac{p(x)}{q(x)}$$

Example: $p(x) = x^3+x^2-1$ and $q(x) = x - 1$

$$\begin{array}{r|l} & x^2 + 2x + 2 \\ \hline x-1 & x^3 + x^2 + 0\cdot x - 1 \\ & -(x^3 - x^2) \\ \hline & 0 + 2x^2 + 0\cdot x - 1 \\ & -(2x^2 - 2x) \\ \hline & 0 + 2x - 1 \\ & -(2x - 2) \\ \hline & 1 \end{array}$$

$q'(x) = x^2 + 2x + 2$

$r(x) = 1$

Proving Property 1

Property 1: A non-zero polynomial of degree d has at most d roots
We will prove this by proving these two other claims.

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
$p(x) = c(x-a_1)\ldots(x-a_d)$ where c is just a number.

Proving Property 1 with Claim 1

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

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

deg 1 $(d-1)$

$$p(x) = (x-a)q(x) + r(x)$$

if a is a root

$$p(a) = 0 = \underbrace{(a-a)}_{=0}\cancel{q(a)} + r(a)$$

0

$$r(a) = 0$$

Proving Property 1 with Claim 2

Property 1: A non-zero polynomial of degree d has at most d roots
Claim 2: A polynomial $p(x)$ of degree d with distinct roots a_1, ..., a_d can be written as $p(x) = c(x-a_1)...(x-a_d)$ where c is just a number.

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

By induction on degree

Ind. Step:

$p(x) = (x - r_1)\, q(x)$ and by Claim 1 $q(x)$ has degree $d-1$

So apply Ind. hyp.

Secret Sharing

There is a code that can be used to launch nuclear weapons.
We don't want this code to be accessed unless k of the total n military generals agree.

How do we solve this?

1284

Secret Sharing (cont.)

There is a secret code that can be used to launch nuclear weapons.
We don't want this code to be accessed unless k of the total n military generals agree.

How do we solve this?

1. Construct a degree k-1 polynomial. Call it $p(x)$.
2. Encode the secret code as $p(0)$ = "*secret code*"
3. Give each general a point that $p(x)$ contains.
   a. i.e. General #1 gets (1, $p(1)$). General #2 gets (2, $p(2)$). So on...
4. When any k general agree. They can share their points and they will have k points to reconstruct a degree k-1 polynomial. Then, they just plug in $p(0)$ to find the secret.

Example of Secret Sharing

Tarang wants to set up a system that if any 3 of Michael, Jingjia, Nikki, Christine, Jet, Colby or Korinna agree then the midterm solutions will be released immediately.

1 2 3 4 5 6 7

Suppose the secret code to the solutions is "6".

What degree polynomial does Tarang need to construct? ___2___

How many points do we need to generate? ___7___ (not including secret)

$p(x) = x^2 + 2x + 6$ $\quad p(0) = 6$ ✓

$GF(7)$

Michael $= (1, p(1)) = (1, 1^2 + 2(1) + 6) = (1, 2)$

Jingjia $= (2, p(2))$ $\quad (2, 0)$

Nikki $= (3, p(3))$ $\quad (3, 0)$

Christine $= (4, p(4))$ $\quad (4, 2)$

⋮ ⋮

Example of Secret Sharing (cont.)

$GF(7)$

Suppose Jingjia, Nikki and Christine agree to release the solutions before the midterm. How would they do it?

Jingjia $(2,0)$
Christine $(4,2)$
Nikki $(3,0)$

$$p(x) = \cancel{\Delta_2 \cdot 0}^{\,0} + \Delta_4 \cdot 2 + \cancel{\Delta_3 \cdot 0}^{\,0}$$

$$\Delta_4 = \frac{(x-2)(x-3)}{(4-2)(4-3)}$$

$$\Delta_4 = 4(x-2)(x-3)$$

$$p(x) = 2 \cdot 4(x-2)(x-3)$$
$$= x^2 + 2x + 6$$

$$p(0) = 6$$

:)

Counting Polynomials

Assume for all these questions we're working in $GF(p)$

How many unique degree at most k polynomials are there?

How many exactly degree k polynomials are there?

If we wish to find a degree 5 polynomial and we know only 3 points how many options do we have for the polynomials that currently go through our 3 points?