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.

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

Polynomials in $GF(p)$

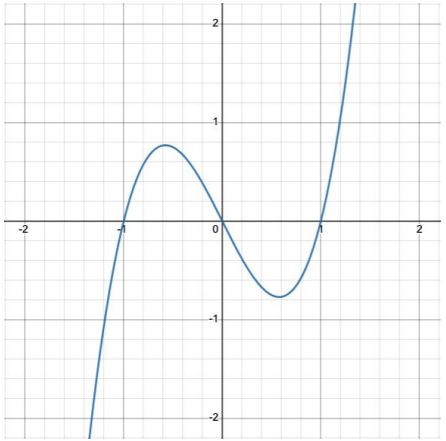
A **polynomial** in $GF(p)$

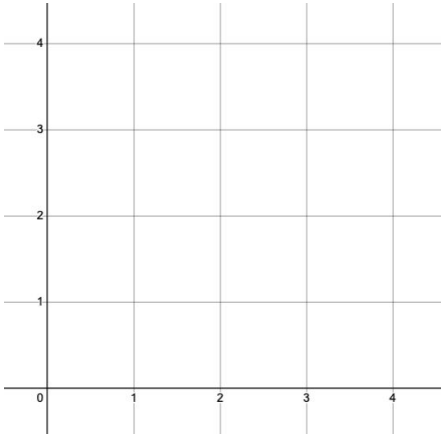
$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

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 $x \in \{0, \ldots, p\text{-}1\}$

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





Polynomials in $GF(p)$

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

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

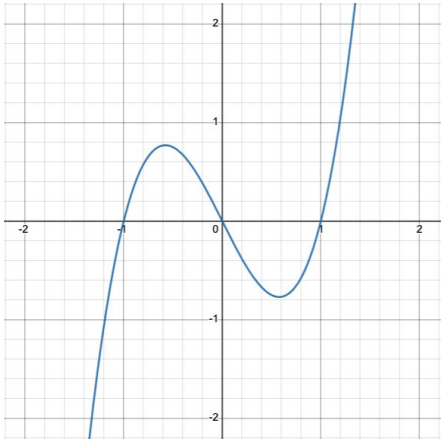
is specified by **coefficients** $a_d, \ldots, a_0$

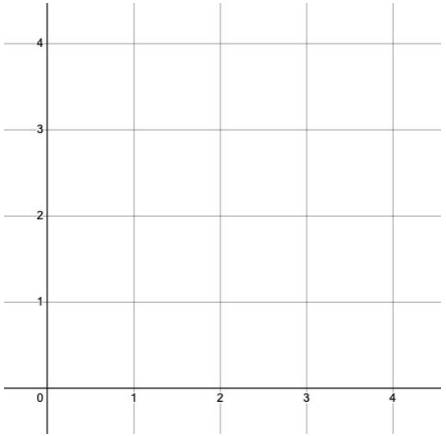
$f(x)$ **contains** point (a, b) if $b = f(a)$

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 $f(a) = 0$

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

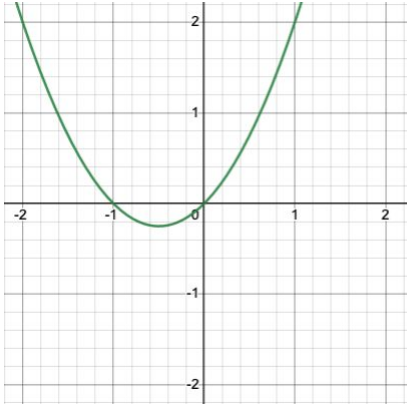


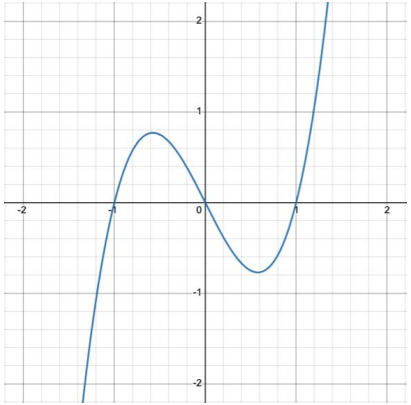


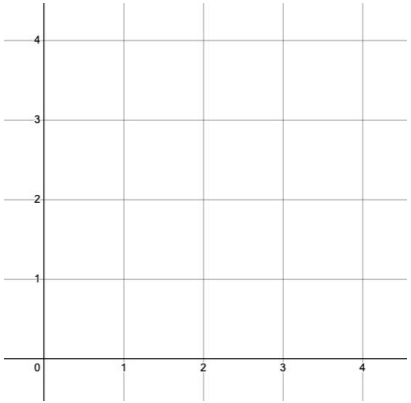
Degree $d \Rightarrow$ at most d roots

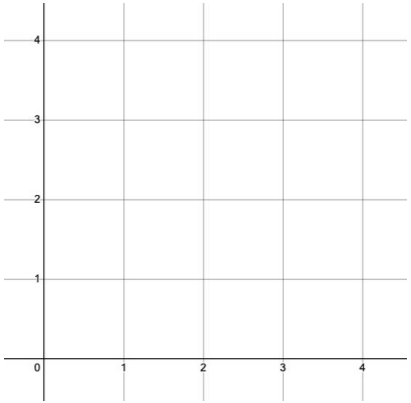
Property 1:
A non-zero polynomial of degree d has at most d roots

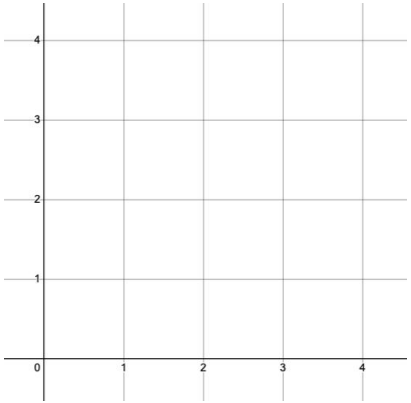
Examples:

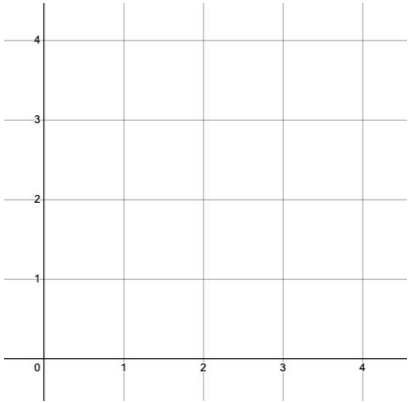












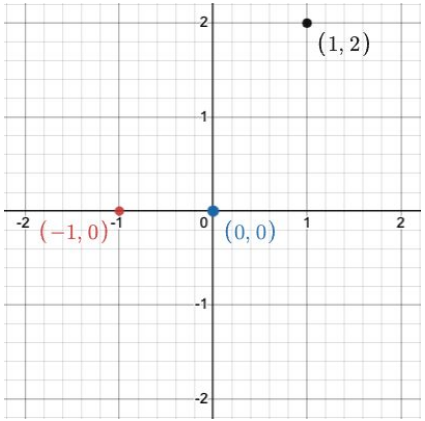
d+1 points $\Rightarrow$ unique degree d polynomial

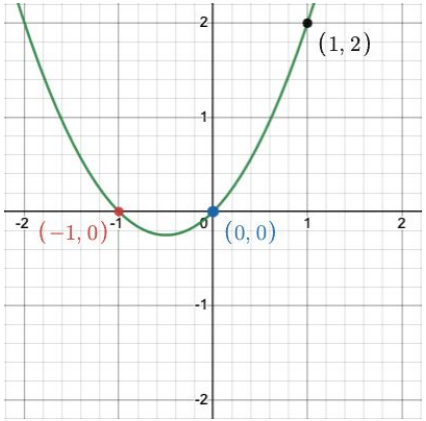
We say a **point** is a x, y pair where $y = f(x)$

<u>Property 2:</u>
Given d+1 pairs: (x_1, y_1), …, (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

Example:





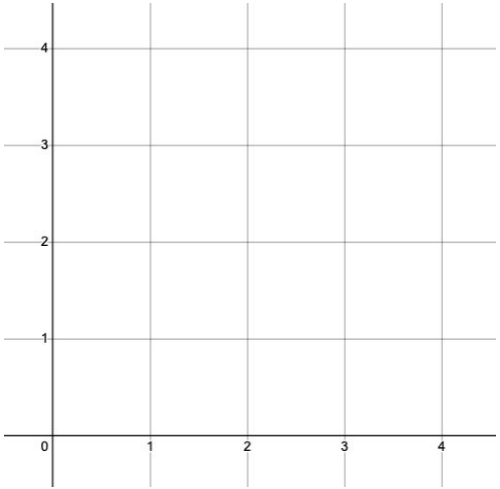
Implication of Properties on a Line

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)



Polynomial Equivalence

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.

Examples in $GF(7)$:

$f_1(x) = x + 1$

$f_2(x) = 8x + 1$

$f_3(x) = x + 8$

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

Polynomials from Points via Interpolation

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

Polynomials from Points via Gaussian Elimination

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

Proving Property 2

Property 2: Given d+1 pairs: (x_1, y_1), …, (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 $1 \leq i \leq d+1$
"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:

Long Division

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

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

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

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 $p(x) = (x-a)q(x)$ for a polynomial $q(x)$ with degree $d - 1$

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 $a_1, \ldots, a_d$ can be written as $p(x) = c(x-a_1)\ldots(x-a_d)$ where c is just a number.

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?

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.
Suppose the secret code to the solutions is “6”.

What degree polynomial does Tarang need to construct? _____

How many points do we need to generate? _____

Example of Secret Sharing (cont.)

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

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?