Polynomial Properties

Def: A polynomial is an expression

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where are called coefficients and is called the variable.

The degree of a polynomial is the largest integer d such that .

Ex: $3x^4 + 2x - 7$ is degree .

We can view polynomials as in .

Ex: $p(x) = 3x^4 + 2x - 7$ can be a function

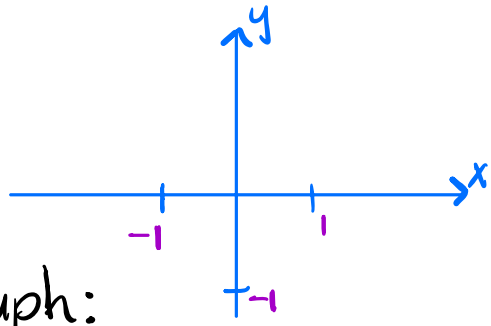
$p: \mathbb{R} \to \mathbb{R}$.

$p(2) =$ $=$

Def: a is a root of $p(x)$ if $p(a) =$.

Ex: $p(x) = x^2 - 1 =$

Roots: $p(1) = p(-1) =$



When viewing $p: \mathbb{R} \to \mathbb{R}$, can graph:

When viewed as functions $\mathbb{R} \to \mathbb{R}$, get two key polynomial properties.

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

Ex: Constant polynomials (degree 0) have zero roots.

$p(x) = 5$ has no roots!

Ex: Parabolas (degree 2)

$p(x) = x^2 - 1$ had 2 roots

$p(x) = x^2$ has 1 root:

$p(x) = x^2 + 1$ has no roots!

Ex: Zero polynomial $p(x) =$ 0 is an exception!

All inputs are roots.

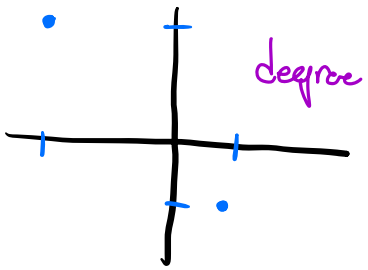
Say degree of zero polynomial is -1 or $-\infty$.

Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ there is a unique polynomial, $p(x)$, of degree d or less passing through them (meaning $p(x_1) = y_1, \ldots, p(x_{d+1}) = y_{d+1}$).

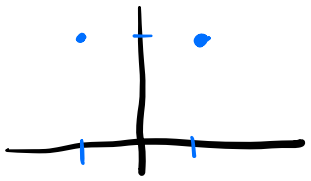
Important: Assume $x_1, \ldots, x_{d+1}$ are distinct.

Ex: Lines (degree 1 or 0)

$(-2, 2), (1, -1)$: $p(x) =$

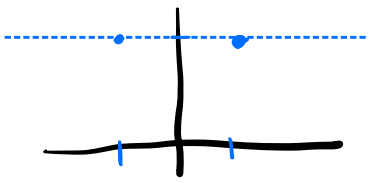


$(-1, 2), (1, 2)$: $p(x) =$



Warning: Other polys on degree ≥ 1 can also pass through these points!

For instance, $p(x) = 2x^2$.



First Goal: Prove two properties.

Start with Property 1.

Polynomial Division

Recall Division Theorem: Given n, m.

Could write $n = q \cdot m + r$ ⟶ remainder

Division Theorem for Polynomials: Given $p(x), s(x)$

we can write $p(x) = q(x) \cdot s(x) + r(x)$ where ↳

degree of r is less than degree of s.

Ex: $p(x) = 3x - 5$, $s(x) = x + 2$

$3x - 5 = \underset{\searrow q(x), \deg}{(x+2)} - \underset{\searrow r(x), \deg}{}$

$p(x) = x^2 - 2x$, $s(x) = x+1$

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

( ): $q(x)$, deg $\quad$ $+$: $r(x)$, deg

More generally, can do long division (see Notes).

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

Proof: To prove this, we will show that if $p(x)$ is degree d and has d roots $a_1, \ldots, a_d$ (distinct), then it can have no other roots.

Lemma: If a_1 is a root of $p(x)$ with degree $d \geq 1$, then $p(x) = (x-a_1)q(x)$ where $q(x)$ is degree $d-1$.

Proof of Lemma: By the Division Theorem with $p(x)$ and $s(x) = x - a_1$, we know

$p(x) = (x-a_1)q(x) + r(x)$ where $r(x)$ has degree 0. So, $r(x) = \;\rightarrow$.

Plugging in a_1,

$= p(a_1) = (a_1 - a_1)q(a_1) + r(a_1) =$.

So, $c=$. Thus, $p(x)=$.

Also, $p(x)$ has degree d so $q(x)$ has degree .

□

Now, consider $p(x)$ of degree d with d roots $a_1, \ldots, a_d$. By the lemma, $p(x) = (x-a_1)q(x)$. $q(x)$ has roots .

Repeat the lemma on $q(x)$, and so on.

Exercise: Do this formally by induction.

Get $p(x) = c(x-a_1)(x-a_2)\cdots(x-a_d)$, $c \neq 0$.

Now, we see that $p(a) \neq$ if a is different from $a_1, \ldots, a_d$.

□

Lagrange Interpolation

Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$.

We will design an algorithm to return a polynomial of degree d or less passing through the points.

Finding this algorithm proves part of Property 2.

Consider points $(x_1, y_1), \ldots, (x_n, y_n)$.

Suppose we made a polynomial $\Delta_{x_i}(x)$ so that

$\Delta_{x_i}(x_i) =$ and $\Delta_{x_i}(x_j) =$ if $i \neq j$.

Then put, $p(x) = \sum_{j=1}^{n} y_j \cdot \Delta_{x_j}(x) = y_1 \cdot \Delta_{x_1}(x) + \cdots + y_n \cdot \Delta_{x_n}(x)$

For each x_i: $p(x_i) =$ $=$. Works!

How to make Δ_{x_i}? Brute force!

Let $Z_{x_i}(x) = (x - x_1) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)$

So, $Z_{x_i}(x_j) =$ when $i \neq j$.

Also, $Z_{x_i}(x_i) \neq$, but... don't know $Z_{x_i}(x_i) = 1$!

Fix: Put $\Delta_{x_i}(x) =$.

Then, $\Delta_{x_i}(x_j) = \frac{Z_{x_i}(x_j)}{Z_{x_i}(x_i)} =$ when $i \neq j$.

$\Delta_{x_i}(x_i) = \frac{Z_{x_i}(x_i)}{Z_{x_i}(x_i)} =$.

This is Lagrange interpolation!

1. Compute $\Delta_{x_i}(x)$ for each i.
2. Put $p(x) = \sum_{j=1}^{n} y_j \cdot \Delta_{x_j}(x)$.

Ex: $(0,-2), (1,1), (3,7)$

$\Delta_0(x) =$ ——— $=$

$\Delta_1(x) =$ ——— $=$

$\Delta_3(x) =$ ——— $=$

$p(x) = \quad \cdot\Delta_0(x) + \quad \cdot\Delta_1(x) + \quad \cdot\Delta_3(x)$

$= -\frac{2}{3}(x-1)(x-3) - \frac{1}{2}x(x-3) + \frac{7}{6}x(x-1)$

$= -\frac{2}{3}x^2 + \frac{8}{3}x - 2 - \frac{1}{2}x^2 + \frac{3}{2}x + \frac{7}{6}x^2 - \frac{7}{6}x$

$=$ $\square$ → polynomial of degree !

Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ there is a unique polynomial, $p(x)$, of degree d or less passing through them.

Proof: $p(x)$ exists via Lagrange interpolation.

Note each $\Delta_{x_i}(x)$ will be degree d, so $p(x)$ will be degree d or less.

We must show uniqueness. Suppose $p(x)$ and $q(x)$ both pass through $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ and are degree d or less. Consider $r(x) =$, which is degree d or less.

Notice $r(x_i) =$ $=$ $=$ for all i. So, $r(x)$ has at roots.

But, recall Property 1: A non-zero polynomial of degree d has at most d roots.

So, $r(x)$ must be the zero polynomial!

So, $p(x) = q(x)$ for all $x \in \mathbb{R}$. They are the same! □

Galois Fields

We want to consider polynomials mod N.

Ideally, we want our two properties to hold.

In the proofs, we used the fact that we could by nonzero real numbers (a.k.a by inverses of nonzero reals).

Def: A field is a number system where you may add, subtract, multiply, and every nonzero number has an inverse.

When is arithmetic mod N a field?

When N is prime! Write $N=p$.

Def: If p is prime, the Galois field mod p is the set $GF(p)=\{0,1,\dots,p-1\}$, where we do arithmetic simplified mod p.

Ex: Polynomials in $GF(3)$.

$p(x)=x^2+2$ GF(3) means work

$p(0)=$, $p(1)=$ $=$ $p(2)=$ $=$

Seems like $p(x)$ has roots at and ...

In fact, $(x-1)(x-2)=$ $=$

Fact: The two polynomial properties hold in $GF(p)$.

Minor Ex: In Lagrange interpolation, we put $\Delta_{x_i}(x)=\frac{Z_{x_i}(x)}{Z_{x_i}(x_i)}$. Now, put $\Delta_{x_i}(x)=Z_{x_i}(x)\left(\quad\right)^{-1}$

1

Confusing Ex: Consider GF(3).

Consider points (0,0), (1,1), (2,2), (3,3)

By Property 2, should be a unique polynomial of degree or less passing through.

$p(x) = x$ works.

$p(x) = x^3$ works too... $p(2) =$, $p(3) =$

Two ways to make sense of this.

1. In GF(3), and are the same point! So only have points.
2. By FLT, $x^3 \equiv$ (mod 3) so the polynomials are the same!

Two important lessons:

1. In GF(p), there are finitely many possible different inputs to a polynomial (and outputs).
2. In GF(p), two polynomials of different degree can be identical on all inputs.

Since options are finite in GF(p), we can count the number of different polynomials.

Ex: In GF(5), how many polynomials of degree 2 or less?

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

options per coefficient: $= \square$ polynomials

Ex: In GF(5), how many polynomials of degree 2 or less that pass through $(0,2)$ and $(2,3)$?

Pick some other input, like 1.

There are possibilities for where 1 maps:

$(1, \ ), (1, \ ), (1, \ ), (1, \ ), (1, \ )$

For each of possible y, there is a unique polynomial of degree 2 or less passing through $(0,2), (1,y), (2,3)$ by Property 2.

Each of these polynomials is distinct since they map 1 to different values.

So, $\square$ possible polynomials.

Fact: In GF(p), there are p^{d-n+1} polynomials of degree d or less passing through a set of $n \leq d+1$ distinct points.

Secret Sharing

Setup: You have a secret, which is an integer $s > 0$.

You have a group of n friends.

Individually, no one should be able to find the secret. But, if $k < n$ work together, they should be able to get the secret.

Procedure: 1. Pick a polynomial $p(x)$ with degree $k-1$ and with $p(0) =$.

2. For each friend 1 to n, give friend i the point $(i, p(i))$.

If k friends get together, they can do Lagrange interpolation to find $q(x)$ of degree

$k-1$ or less that passes through all their points.

But: $p(x)$ is degree and passes through their points! By uniqueness in Property 2, $q(x) =$! So, they can get the secret.

If a smaller group of friends does Lagrange interpolation and gets $q(x)$, then $q(0)$ could be anything! Can't get secret.

Often, we want to do this in $GF(p)$ for some prime p so we can work with integers.

Make sure: $p >$ (else secret is cut off)

$p >$ (else not enough distinct points to give out!)