

Today.

Polynomials.

Secret Sharing.

Correcting for loss or even corruption.

Secret Sharing.

Share secret among n people.

Secrecy: Any $k - 1$ knows nothing.

Robustness: Any k knows secret.

Efficient: minimize storage.

The idea of the day.

Two points make a line.

Lots of lines go through one point.

Polynomials

A polynomial

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

is specified by **coefficients** a_d, \dots, a_0 .

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

Polynomials over reals: $a_1, \dots, a_d \in \mathfrak{R}$, use $x \in \mathfrak{R}$.

Polynomials $P(x)$ with arithmetic modulo p :¹ $a_i \in \{0, \dots, p-1\}$
and

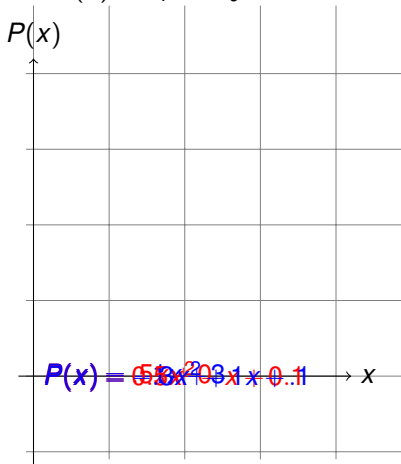
$$P(x) = a_d x^d + a_{d-1} x^{d-1} \dots + a_0 \pmod{p},$$

for $x \in \{0, \dots, p-1\}$.

¹A field is a set of elements with addition and multiplication operations, with inverses. $GF(p) = (\{0, \dots, p-1\}, + \pmod{p}, * \pmod{p})$.

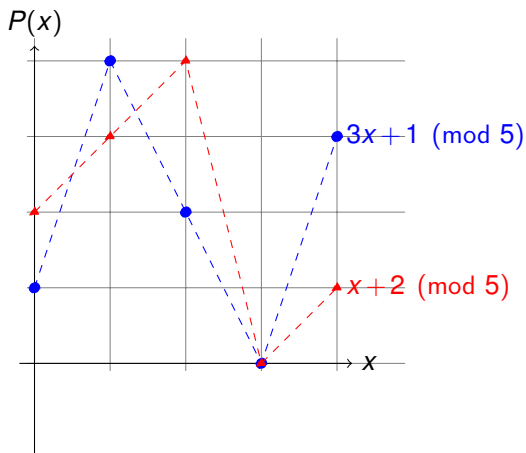
Polynomial: $P(x) = a_d x^d + \dots + a_0$

Line: $P(x) = a_1 x + a_0 = mx + b$



Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

Polynomial: $P(x) = a_d x^d + \dots + a_0 \pmod{p}$



Finding an intersection.

$$x + 2 \equiv 3x + 1 \pmod{5}$$

$$\implies 2x \equiv 1 \pmod{5} \implies x \equiv 3 \pmod{5}$$

3 is multiplicative inverse of 2 modulo 5.

Good when modulus is prime!!

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d + 1$ points. ²

Two points specify a line. Three points specify a parabola.

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d + 1$ pts.

²Points with different x values.

Poll.

Two points determine a line.

What facts below tell you this?

Say points are $(x_1, y_1), (x_2, y_2)$.

(A) Line is $y = mx + b$.

(B) Plug in a point gives an equation: $y_1 = mx_1 + b$

(C) The unknowns are m and b .

(D) If equations have unique solution, done.

All true.

Flow Poll.

Why solution? Why unique?

- (A) Solution cuz: $m = (y_2 - y_1)/(x_2 - x_1)$, $b = y_1 - m(x_1)$
- (B) Unique cuz, only one line goes through two points.
- (C) Try: $(m'x + b') - (mx + b) = (m' - m)x + (b - b) = ax + b \neq 0$.
- (D) Either $ax_1 + c \neq 0$ or $ax_2 + c \neq 0$.
- (E) Contradiction.

Flow poll. (All true. (B) is not a proof, it is restatement.)

Notation: two points on a line.

Polynomial: $a_n x^n + \dots + a_0$.

Consider line: $mx + b$

(A) $a_1 = m$

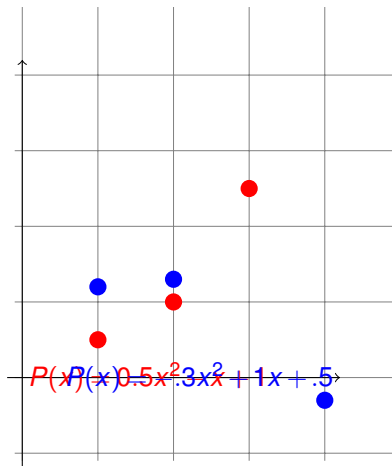
(B) $a_1 = b$

(C) $a_0 = m$

(D) $a_0 = b$.

(A) and (D)

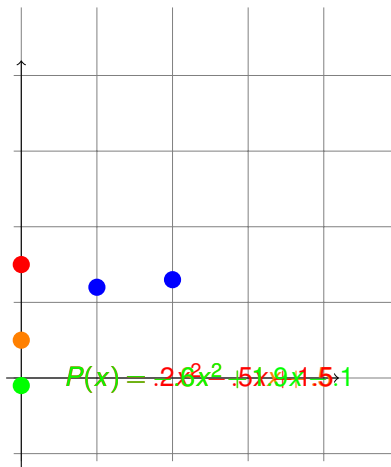
3 points determine a parabola.



Fact: Exactly 1 degree $\leq d$ polynomial contains $d + 1$ points. ³

³Points with different x values.

2 points not enough.



There is $P(x)$ contains blue points and *any* $(0, y)$!

Modular Arithmetic Fact and Secrets

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d + 1$ pts.

Shamir's k out of n Scheme:

Secret $s \in \{0, \dots, p-1\}$

1. Choose $a_0 = s$, and random a_1, \dots, a_{k-1} .
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_0$ with $a_0 = s$.
3. Share i is point $(i, P(i) \bmod p)$.

Roubustness: Any k shares gives secret.

Knowing k pts \implies only one $P(x) \implies$ evaluate $P(0)$.

Secrecy: Any $k - 1$ shares give nothing.

Knowing $\leq k - 1$ pts \implies any $P(0)$ is possible.

From $d + 1$ points to degree d polynomial?

For a line, $a_1x + a_0 = mx + b$ contains points $(1, 3)$ and $(2, 4)$.

$$P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}$$

$$P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5}$$

Subtract first from second..

$$m + b \equiv 3 \pmod{5}$$

$$m \equiv 1 \pmod{5}$$

Backsolve: $b \equiv 2 \pmod{5}$. **Secret is 2.**

And the line is...

$$x + 2 \pmod{5}.$$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1, 2); (2, 4); (3, 0)$.
Plug in points to find equations.

$$P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}$$

$$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}$$

$$P(3) = 9a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}$$

$$a_2 + a_1 + a_0 \equiv 2 \pmod{5}$$

$$3a_1 + 2a_0 \equiv 1 \pmod{5}$$

$$4a_1 + 2a_0 \equiv 2 \pmod{5}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.

$$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod{5}$$

$$a_2 = 2 - 1 - 4 \equiv 2 \pmod{5}.$$

So polynomial is $2x^2 + 1x + 4 \pmod{5}$

In general..

Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)$.

Solve...

$$a_{k-1}x_1^{k-1} + \cdots + a_0 \equiv y_1 \pmod{p}$$

$$a_{k-1}x_2^{k-1} + \cdots + a_0 \equiv y_2 \pmod{p}$$

.

.

$$a_{k-1}x_k^{k-1} + \cdots + a_0 \equiv y_k \pmod{p}$$

Will this always work?

As long as solution **exists** and it is **unique!** And...

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d + 1$ pts.

Another Construction: Interpolation!

For a quadratic, $a_2x^2 + a_1x + a_0$ hits $(1, 3); (2, 4); (3, 0)$.

Find $\Delta_1(x)$ polynomial contains $(1, 1); (2, 0); (3, 0)$.

Try $(x-2)(x-3) \pmod{5}$.

Value is 0 at 2 and 3. Value is 2 at 1. **Not 1! Doh!!**

So "Divide by 2" or multiply by 3.

$\Delta_1(x) = (x-2)(x-3)(3) \pmod{5}$ contains $(1, 1); (2, 0); (3, 0)$.

$\Delta_2(x) = (x-1)(x-3)(4) \pmod{5}$ contains $(1, 0); (2, 1); (3, 0)$.

$\Delta_3(x) = (x-1)(x-2)(3) \pmod{5}$ contains $(1, 0); (2, 0); (3, 1)$.

But wanted to hit $(1, 3); (2, 4); (3, 0)$!

$P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?

...after a lot of calculations... $P(x) = 2x^2 + 1x + 4 \pmod{5}$.

The same as before!

Fields.. .

Flowers, and grass, oh so nice.

Set and two commutative operations: addition and multiplication with additive/multiplicative identities and inverses except for additive identity has no multiplicative inverse.

E.g., Reals, rationals, complex numbers.

Not E.g., the integers, matrices.

We will work with polynomials with arithmetic modulo p .

Addition is cool. Inherited from integers and integer division (remainders).

Multiplicative inverses due to $\gcd(x, p) = 1$, for all $x \in \{1, \dots, p-1\}$

Delta Polynomials: Concept.

For set of x -values, x_1, \dots, x_{d+1} .

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

Given $d + 1$ points, use Δ_i functions to go through points?

$(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$.

Will $y_1 \Delta_1(x)$ contain (x_1, y_1) ?

Will $y_2 \Delta_2(x)$ contain (x_2, y_2) ?

Does $y_1 \Delta_1(x) + y_2 \Delta_2(x)$ contain
 (x_1, y_1) ? and (x_2, y_2) ?

See the idea? Function that contains all points?

$P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) \dots + y_{d+1} \Delta_{d+1}(x)$.

There exists a polynomial...

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d + 1$ pts.

Proof of at least one polynomial:

Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

$$\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} = \prod_{j \neq i} (x - x_j) \prod_{j \neq i} (x_i - x_j)^{-1}$$

Numerator is 0 at $x_j \neq x_i$.

“Denominator” makes it 1 at x_i .

And..

$$P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + \cdots + y_{d+1} \Delta_{d+1}(x).$$

hits points $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$. Degree d polynomial!

Construction proves the existence of a polynomial!

Poll

Mark what's true.

(A) $\Delta_1(x_1) = y_1$

(B) $\Delta_1(x_1) = 1$

(C) $\Delta_1(x_2) = 0$

(D) $\Delta_1(x_3) = 1$

(E) $\Delta_1(x_2) = 1$

(F) $\Delta_2(x_1) = 0$

(B), (C), and (E)

Example.

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

Degree 1 polynomial, $P(x)$, that contains $(1, 3)$ and $(3, 4)$?

Work modulo 5.

$\Delta_1(x)$ contains $(1, 1)$ and $(3, 0)$.

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

$$\begin{aligned}\Delta_1(x) &= (x-3)(1-3)^{-1} = (x-3)(-2)^{-1} \\ &= 2(x-3) = 2x-6 = 2x+4 \pmod{5}.\end{aligned}$$

For a quadratic, $a_2x^2 + a_1x + a_0$ hits $(1, 3); (2, 4); (3, 0)$.

Work modulo 5.

Find $\Delta_1(x)$ polynomial contains $(1, 1); (2, 0); (3, 0)$.

$$\begin{aligned}\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = (2)^{-1}(x-2)(x-3) = 3(x-2)(x-3) \\ &= 3x^2 + 3 \pmod{5}\end{aligned}$$

Put the delta functions together.

In general.

Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)$.

$$\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} = \prod_{j \neq i} (x - x_j) \prod_{j \neq i} (x_i - x_j)^{-1}$$

Numerator is 0 at $x_j \neq x_i$.

Denominator makes it 1 at x_i .

And..

$$P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + \cdots + y_k \Delta_k(x).$$

hits points $(x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)$.

Construction proves the existence of the polynomial!

Uniqueness.

Uniqueness Fact. At most one degree d polynomial hits $d + 1$ points.

Roots fact: Any nontrivial degree d polynomial has at most d roots.

Non-zero line (degree 1 polynomial) can intersect $y = 0$ at only one x .

A parabola (degree 2), can intersect $y = 0$ at only two x 's.

Proof:

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

$R(x) = Q(x) - P(x)$ has $d + 1$ roots and is degree d .

Contradiction.



Must prove **Roots fact**.

Only d roots.

Lemma 1: $P(x)$ has root a iff $P(x)/(x - a)$ has remainder 0:
 $P(x) = (x - a)Q(x)$.

Proof: $P(x) = (x - a)Q(x) + r$.

Plugin a : $P(a) = r$.

It is a root if and only if $r = 0$.



Lemma 2: $P(x)$ has d roots; r_1, \dots, r_d then
 $P(x) = c(x - r_1)(x - r_2) \cdots (x - r_d)$.

Proof Sketch: By induction.

Induction Step: $P(x) = (x - r_1)Q(x)$ by Lemma 1. $Q(x)$ has smaller degree so use the induction hypothesis.



$d + 1$ roots implies degree is at least $d + 1$.

Roots fact: Any degree d polynomial has at most d roots.

Finite Fields

Proof works for reals, rationals, and complex numbers.

..but not for integers, since no multiplicative inverses.

Arithmetic modulo a prime p has multiplicative inverses..

..and has only a finite number of elements.

Good for computer science.

Arithmetic modulo a prime m is a **finite field** denoted by F_m or $GF(m)$.

Intuitively, a field is a set with operations corresponding to addition, multiplication, and division.

Secret Sharing

Modular Arithmetic Fact: Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d + 1$ points.

Shamir's k out of n Scheme:

Secret $s \in \{0, \dots, p - 1\}$

1. Choose $a_0 = s$, and randomly a_1, \dots, a_{k-1} .
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_0$ with $a_0 = s$.
3. Share i is point $(i, P(i) \bmod p)$.

Robustness: Any k knows secret.

Knowing k pts, only one $P(x)$, evaluate $P(0)$.

Secrecy: Any $k - 1$ knows nothing.

Knowing $\leq k - 1$ pts, any $P(0)$ is possible.

Minimality.

Need $p > n$ to hand out n shares: $P(1) \dots P(n)$.

For b -bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Chebyshev said it,

And I say it again,

There is always a prime

Between n and $2n$.

Working over numbers within 1 bit of secret size. **Minimality.**

With k shares, reconstruct polynomial, $P(x)$.

With $k - 1$ shares, any of p values possible for $P(0)$!

(Almost) any b -bit string possible!

(Almost) the same as what is missing: one $P(i)$.

Runtime.

Runtime: polynomial in k , n , and $\log p$.

1. Evaluate degree $k - 1$ polynomial n times using $\log p$ -bit numbers.
2. Reconstruct secret by solving system of k equations using $\log p$ -bit arithmetic.

A bit more counting.

What is the number of degree d polynomials over $GF(m)$?

- ▶ m^{d+1} : $d + 1$ coefficients from $\{0, \dots, m - 1\}$.
- ▶ m^{d+1} : $d + 1$ points with y -values from $\{0, \dots, m - 1\}$

Infinite number for reals, rationals, complex numbers!

Summary

Two points make a line.

Compute solution: m, b .

Unique:

Assume two solutions, show they are the same.

Today: $d + 1$ points make a unique degree d polynomial.

Cuz:

Solution: lagrange interpolation.

Unique:

Roots fact: Factoring sez $(x - r)$ is root.

Induction, says only d roots.

Apply: $P(x), Q(x)$ degree d .

$P(x) - Q(x)$ is degree $d \implies d$ roots.

$P(x) = Q(x)$ on $d + 1$ points $\implies P(x) = Q(x)$.

Secret Sharing:

k points on degree $k - 1$ polynomial is great!

Can hand out n points on polynomial as shares.