Polynomials

Today.

Secret Sharing.

Polynomials.

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.

Polynomial: \( P(x) = a_dx^4 + \cdots + a_0 \)

Line: \( \text{Line}(x) = a_1 x + a_0 = mx + b \)

Parabola: \( \text{Parabola}(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c \)

Polynomial: \( P(x) = a_dx^4 + \cdots + a_0 \pmod{p} \)

Finding an intersection.

\( x + 2 \equiv 3x + 1 \pmod{5} \)

\( \Rightarrow 2x \equiv 1 \pmod{5} \)

\( \Rightarrow x \equiv 3 \pmod{5} \)

3 is multiplicative inverse of 2 modulo 5.

Good when modulus is prime!!

Polynomials

A polynomial

\[ P(x) = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_0 \]

is specified by coefficients \( a_0, \ldots, a_d \).

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

Polynomials over reals: \( a_1, \ldots, a_d \in \mathbb{R} \), use \( x \in \mathbb{R} \).

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

\[ P(x) = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_0 \pmod{p}, \]

for \( x \in \{0, \ldots, p-1\} \).

Two points make a line.

Fact: Exactly 1 degree \( \leq d \) polynomial contains \( d+1 \) points.

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.

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

\(^2\)Points with different \( x \) values.
3 points determine a parabola.

\[ P(x) = 0.5x^2 - x + 1 \]

Fact: Exactly 1 degree \( \leq d \) polynomial contains \( d + 1 \) points. \(^3\)

\(^3\)Points with different \( x \) values.

2 points not enough.

\[ P(x) = -0.3x^2 + x + 0.5 \]

For a quadratic polynomial, \( a_2x^2 + a_1x + a_0 \) hits \((1,2),(2,4)\).

Plug in points to find equations.

\[
\begin{align*}
P(1) &= a_2 + a_1 + a_0 = 2 & \pmod{5} \\
P(2) &= 4a_2 + 2a_1 + a_0 = 4 & \pmod{5} \\
P(3) &= 4a_2 + 3a_1 + a_0 = 0 & \pmod{5}
\end{align*}
\]

Subtract first from second.

\[
\begin{align*}
m + b &= 3 & \pmod{5} \\
m &= 1 & \pmod{5}
\end{align*}
\]

Backsolve: \( b = 2 \pmod{5} \). Secret is 2.

And the line is... \( x + 2 \pmod{5} \).

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:**

- Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
- Let \( P(x) = a_0x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \) with \( a_0 = s \).
- Share \( k \) out of \( n \) points.

**Roubustness:** Any \( k \) shares gives secret.

**Secrecy:** Any \( k - 1 \) shares give nothing.

In general...

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

Solve...

\[
\begin{align*}
a_{k-1}x_1^{k-1} + \cdots + a_0 &= y_1 & \pmod{p} \\
a_{k-1}x_2^{k-1} + \cdots + a_0 &= y_2 & \pmod{p} \\
\cdots \\
a_{k-1}x_k^{k-1} + \cdots + a_0 &= y_k & \pmod{p}
\end{align*}
\]

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 $(x - 2)(x - 3) = (x - 1)(x - 3)(3) (mod 5)$.

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

So “Divide by 2” or multiply by 3.

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

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

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... $P(x) = 2x^2 + 1x + 4 \mod 5$.

The same as before!

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: $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$.

$\Delta_i(x) = \prod_{j=2}^{d+1}(x - x_j) \prod_{j=1}^{d+1}(x - x_j)^{-1}$

Numerator is 0 at $x_i \neq x_i$.

“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 $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$. Degree $d$ polynomial!

Construction proves the existence of a polynomial!

**Example.**

$\Delta_1(x) = \prod_{i=2}^{d+1}(x - x_i)$

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

Work modulo 5.

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

$\Delta_1(x) = \frac{x - 1}{x - 3} \frac{x - 3}{x - 2} = \frac{2x - 2}{x - 2} (mod 5)$.

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 $(1,1); (2,0); (3,0)$.

$\Delta_1(x) = \frac{2x - 2}{x - 2} (mod 5)$.

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

$= 3x^2 + 3 \ (mod 5)$

Put the delta functions together.

**Delta Polynomials: Concept.**

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

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

Given $d + 1$ points, use $\Delta_i$ functions to go through points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$.

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?

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

**In general.**

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

$\Delta_i(x) = \frac{\prod_{j=2}^{d+1}(x - x_j)}{\prod_{j=1}^{d}(x - x_j)} \prod_{j=1}^{d}(x - x_j)^{-1}$

Numerator is 0 at $x_i \neq x_i$.

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 $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$.

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.

Polynomial Division.

Divide $4x^2 - 3x + 2$ by $(x - 3)$ modulo 5.

<table>
<thead>
<tr>
<th>4x + 4</th>
<th>r</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>x - 3</td>
<td>4x^2 - 3x + 2</td>
<td>4x^2 - 2x</td>
</tr>
<tr>
<td>4x + 2</td>
<td>4x - 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

$4x^2 - 3x + 2 \equiv (x - 3)(4x + 4) + 4 \mod 5$

In general, divide $P(x)$ by $(x - a)$ gives $Q(x)$ and remainder $r$.
That is, $P(x) = (x - a)Q(x) + r$

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; $r_1, \ldots, r_d$ then
$P(x) = c(x - r_1)(x - r_2) \cdots (x - r_d)$.
Proof Sketch: By induction.
Induction Step: $P(x) = (x - r_i)Q(x)$ 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.