
1. Finish Polynomials and Secrets.
2. Finite Fields: Abstract Algebra
3. Erasure Coding

Reiterating Examples.

\[ \Delta_i(x) = \prod_{j \neq i} (x - x_j) \]
Degree 1 polynomial, \( P(x) \), that contains \( (1,3) \) and \( (3,4) \)?

Work modulo 5.

\[ \Delta_1(x) = \prod_{j \neq 1} (x - x_j) = \prod_{j \neq 1} (x - 2x_j) = 2 \] (mod 5).

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

Work modulo 5.

\[ \Delta_1(x) \text{ polynomial contains } (1,1); (2,0); (3,0). \]

\[ \Delta_1(x) = \frac{1}{3}(-2a_1x^2 + 2 = 3(x-2)(x-3) = 3x^2 + 1 \] (mod 5).

Put the delta functions together.

Modular Arithmetic Fact and Secrets

**Modular Arithmetic Fact:** There is exactly 1 polynomial of degree \( \leq d \) with arithmetic modulo prime \( p \) that contains \( d+1 \) pts.

Note: The points have to have different \( x \) values!

**Shamir’s \( k \) out of \( n \) Scheme:**

\[ a = \prod_{j \neq i} (x - x_j) \]
1. Choose \( a_0 \) = \( s \), and random \( a_1, \ldots, a_{n-1} \).
2. Let \( P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \) with \( a_0 = s \).
3. Share \( i \) is point \( (i, P(i) \mod p) \).

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

Knowing \( k \) pts, find unique \( P(x) \), evaluate \( P(0) \).

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

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

Simultaneous Equations Method.

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

\[ P(1) = m + b = 3 \] (mod 5)
\[ P(2) = 2m + b = 4 \] (mod 5)

Subtract first from second.

\[ m + b = 3 \] (mod 5)
\[ m = 1 \] (mod 5)

Backsolve: \( b = 2 \) (mod 5). Secret is 2.

And the line is...

\[ x + 2 \] (mod 5).

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

\[ \Delta_i(x) = \prod_{j \neq i} (x - x_j) \]

Numerator is 0 at \( x \).

Denominator makes it 1 at \( x \).

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!

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.

\[ P(1) = a_2 + a_1 + a_0 = 2 \] (mod 5)
\[ P(2) = 4a_2 + 2a_1 + a_0 = 4 \] (mod 5)
\[ P(3) = 4a_2 + 3a_1 + a_0 = 0 \] (mod 5)
\[ a_2 + a_1 + a_0 = 2 \] (mod 5)
\[ 3a_2 + 2a_1 = 1 \] (mod 5)
\[ 4a_2 + 2a_1 = 2 \] (mod 5)

Subtracting 2nd from 3rd yields: \( a_1 = 1 \).

\[ a_2 = \frac{(2 - 4)(a_1)}{2} = -2 \] (mod 5)
\[ a_2 = 2 - 4 = 2 \] (mod 5).

So polynomial is \( 2x^2 + x + 4 \) (mod 5).
Uniqueness.

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

Existence: Lagrange interpolation. Uniqueness?

Uniqueness Fact. At most one degree $d$ polynomial contains $d+1$ pts.

Proof:

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

Assume two different polynomials $Q(x)$ and $P(x)$ hits $d+1$ 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:

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

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

Plugin $a$: $P(a) = r = 0$.

Lemma 2: $P(x)$ has $d$ roots; $r_1,...,r_d$ then

$P(x) = (x-r_1)(x-r_2)\cdots(x-r_d)Q(x)$.

Proof Sketch: By induction.

Base Case: degree 0. No roots.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1. $Q(x)$ has smaller degree...

so by induction hypothesis...

we are done.

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

The contrapositive...

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

Summary.

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

Existence: Lagrange Interpolation.

Uniqueness: At most $d$ roots for degree $d$ polynomial.

In general.

Given points: $(x_1,y_1);(x_2,y_2),\ldots,(x_d,y_d)$.

Solve...

$\begin{align*}
a_0 \cdot x^d + \cdots + a_0 &= y_1 \pmod{p} \\
a_0 \cdot x^d + \cdots + a_0 &= y_2 \pmod{p} \\
&\vdots \\
a_0 \cdot x^d + \cdots + a_0 &= y_0 \pmod{p}
\end{align*}$

Will this always work?

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

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

Polynomial Division.

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

$\begin{align*}
4x + 4 &\equiv 4 \\
\begin{array}{c|c|c|c|c|c|c|c|c|c|c}
x - 3 & 4x^2 & - 3x & + 2 \\
\hline
4x^2 & - 2x \\
\hline
4x & + 2 \\
4x & - 2 \\
\hline
4
\end{array}
\end{align*}$

$4x^2 - 3x + 2 \equiv (x-3)(4x + 4) + 4 \pmod{5}$

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

That is, $P(x) = (x-a)Q(x) + r$

$r$ is degree 0 polynomial..or a constant!
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 $p$ is a finite field denoted by $F_p$ or $GF(p)$.

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:

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$. Evaluate $P(0)$.
3. Share $i$ is point $(i, P(i) \mod p)$.

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.

Efficiency: ???
Problem: Want to send a message with \( n \) packets.
Channel: Lossy channel: loses \( k \) packets.
Question: Can you send \( n + k \) packets and recover message?
On Friday!