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

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:**

\[ \text{Secret } s \in \{0, \ldots, p-1\} \]

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{n-1} \).
2. Let \( P(x) = a_0 x^{d-1} + a_1 x^{d-2} + \cdots + a_d \) with \( a_0 = s \).
3. Share \( f/i \) for \( i \geq 1 \) 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.

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 \( x_j \neq x_i \).

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

Construction proves the existence of a polynomial!

Reiterating Examples.

\[ \Delta(x) = \prod_{j \neq k} \frac{x-x_j}{x-x_k} \]

Degree 1 polynomial, \( P(x) \), that contains \((1,3)\) and \((2,4)\)?

Work modulo 5.

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

\[ \Delta_1(x) = \frac{x-2}{x-1} - \frac{x-3}{x-1} = \frac{2x-3}{x-1} = 2x - 6 - 2x + 4 \mod 5 \]

For a quadratic, \( a_2 x^2 + a_1 x + a_0 \) hits \((1,3);(2,4);(3,0)\).

Work modulo 5.

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

\[ \Delta_1(x) = \frac{1-2(x-2)}{x-3} = \frac{1-2x+4}{x-3} = 3(x-2)(x-3) = 3x^2 + 1 \mod 5 \]

Put the delta functions together.

Simultaneous Equations Method.

For a line, \( a_1 x + a_0 = mx + b \) contains points \((1,3)\) and \((2,4)\).

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

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

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...

\[ x + 2 \mod 5 \]

Quadratic

For a quadratic polynomial, \( a_2 x^2 + a_1 x + a_0 \) hits \((1,2);(2,4);(3,0)\).

Plug in points to find equations.

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

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

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

\[ a_0 + a_1 + a_2 = 2 \mod 5 \]

\[ 3a_0 + 2a_1 = 1 \mod 5 \]

\[ 4a_0 + 2a_1 = 2 \mod 5 \]

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

\[ a_0 = (2-4a_1)2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 = 4 \mod 5 \]

\[ a_2 = 2 - 4 = 2 \mod 5 \]

So polynomial is \( 2x^2 + 1x + 4 \mod 5 \)
In general.

Given points: \((x_1, y_1); (x_2, y_2) \cdot \cdot \cdot (x_n, y_n)\).
Solve...

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

Will this always work?
As long as solution exists and it is unique! And...

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

Summary.

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

Existence:
- Lagrange Interpolation.

Uniqueness: (proved last time)
- At most \(d\) roots for degree \(d\) polynomial.

Efficiency.

Need \(p > n\) to hand out \(n\) shares: \(P(1) \ldots P(n)\).
For \(b\)-bit secret, must choose a prime \(p > 2^b\).
Theorem: There is always a prime between \(n\) and \(2n\).
Working over numbers within 1 bit of secret size. Minimal!
With \(k\) shares, reconstruct polynomial, \(P(x)\).
With \(k – 1\) shares, any of \(p\) values possible for \(P(0)\)?
(Within 1 bit of) any \(b\)-bit string possible!
(Within 1 bit of) \(b\)-bits are missing: one \(P(i)\).
Within 1 of optimal number of bits.

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.

Runtime.

Runtime: polynomial in \(k\), \(n\), and \(\log p\).
1. Evaluate degree \(n\) polynomial \(n + k\) times using \(\log p\)-bit numbers. \(O(k\log^2 p)\).
2. Reconstruct secret by solving system of \(n\) equations using \(\log p\)-bit arithmetic. \(O(n\log^2 p)\).
3. Matrix has special form so \(O(n\log n\log^2 p)\) reconstruction.
Faster versions in practice are almost as efficient.

Secret Sharing Revisited

**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 \(s \in \{0, \ldots , p - 1\}\)
  1. Choose \(a_0 = s\), and random \(a_1, \ldots , a_{n-1}\).
  2. Let \(P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}\) with \(a_0 = s\).
  3. Share \(i\) is point \((i, P(i)) \pmod p\).

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: ???
### A bit of counting.

What is the number of degree $d$ polynomials over $GF(m)$?
- $m^{d+1}$: $d + 1$ coefficients from $\{0, \ldots, m - 1\}$.
- $m^{d+1}$: $d + 1$ points with $y$-values from $\{0, \ldots, m - 1\}$

Infinite number for reals, rationals, complex numbers!

### Solution Idea.

- $n$ packet message, channel that loses $k$ packets.
- Must send $n + k$ packets!
- Any $n$ packets should allow reconstruction of $n$ packet message.
- Any $n$ point values allow reconstruction of degree $n - 1$ polynomial which has $n$ coefficients!
- Alright!!!
- Use polynomials.

---

### Erasure Codes.

**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?

**Solution Idea:** Use Polynomials!!!

- Use polynomials

---

**Solution Idea.**

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!
Any $n$ packets should allow reconstruction of $n$ packet message.
Any $n$ point values allow reconstruction of degree $n - 1$ polynomial which has $n$ coefficients!
Alright!!!
Use polynomials.

---

### Erasure Codes.

**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?

A degree $n - 1$ polynomial determined by any $n$ points!

Erasure Coding Scheme: message = $m_0, m_1, m_2, \ldots, m_{n-1}$. Each $m_i$ is a packet.

1. Choose prime $p > 2^b$ for packet size $b$ (size = number of bits).
2. $P(x) = m_0 + x^{n-1} + \cdots + m_0 \pmod{p}$.
3. Send $P(1), \ldots, P(n + k)$.

Any $n$ of the $n + k$ packets gives polynomial ...and message!

---

**Solution Idea.**

$n$ packet message. So send $n + k$!

**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?

Any $n$ packets is enough!

$n$ packet message.
Optimal.
Comparison with Secret Sharing.

Comparing information content:
Secret Sharing: each share is size of whole secret.
Coding: Each packet has size \( \frac{1}{n} \) of the whole message.

Erasure Code: Example.
Send message of 1, 4, and 4 up to 3 erasures. \( n = 3, k = 3 \)
Make polynomial with \( P(1) = 1, P(2) = 4, P(3) = 4 \).
How?
Lagrange Interpolation.
Linear System.
Work modulo 5.
\[
P(x) = x^2 \quad (\text{mod } 5)
\]
\[
P(1) = 1, P(2) = 4, P(3) = 9 - 4 \quad (\text{mod } 5)
\]
Send \((0, P(0))\) ... \((5, P(5))\).
6 points. Better work modulo 7 at least!
Why?
\[
(0, P(0)) = (5, P(5)) \quad (\text{mod } 5)
\]

Summary: Polynomials are useful!

▶ give Secret Sharing.
▶ give Erasure Codes.

Next time: correct broader class of errors!