Today.

Polynomials.
Secret Sharing.
Erasure Coding.

Back to secret sharing: idea of the day

Two points make a line.
Lots of lines go through one point.
Secret message is represented as the y-intercept.
Let’s recall how polynomials work.

Secret Sharing.

Share secret among \( n \) people.
Secrecy: Any \( k - 1 \) knows nothing.
Robustness: Any \( k \) knows secret.
Efficient: Minimize storage.

Illustration: need at least 3 keys to open a bank vault

Polynomials

A polynomial
\[ P(x) = \sum_{i=0}^{d} a_i x^i \]
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
\[ P(x) = \sum_{i=0}^{d} a_i x^i \pmod{p}, \]
for \( x \in \{0, \ldots, p-1\} \).

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

Other apps. we’ll see: codes based on polynomials

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

Line:
\[ P(x) = a_1 x + a_0 = mx + b \]

Parabola:
\[ P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c \]
Two points make a line.

Fact: There is exactly 1 polynomial having degree \( \leq d \) containing \( d + 1 \) points. Two points specify a line. Three points specify a parabola.

Modular Arithmetic Fact: There is exactly 1 polynomial having degree \( \leq d \) (with arithmetic modulo prime \( p \)) containing \( d + 1 \) pts.

3 points determine a parabola.

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

Question: How many parabolas exist that contain exactly 2 distinct points?

A parabola \( P(x) \) containing 2 blue points can contain any \((0,y)\)!

Modular Arithmetic Fact and Secrets

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

Shamir’s \( k \) out of \( n \) Scheme:
Secret \( s \in \{0,\ldots,p-1\} \)
1. Choose \( a_0 = s \), and random \( a_1,\ldots,a_{d-1} \).
2. Let \( P(x) = a_{d-1}x^d + \cdots + a_1x + a_0 \) with \( a_0 = s \).
3. Share \( i \) is point \((i,P(i)) \mod p\).

Robustness: 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, \( a_1 x + a_0 = mx + b \) contains points \((1,3)\) and \((2,4)\).
\[
P(1) = m(1) + b = m + b \equiv 3 \pmod{5}
\]
\[
P(2) = m(2) + b = 2m + b \equiv 4 \pmod{5}
\]

Subtract first from second.
\[
m + b = 3 \pmod{5}
\]
\[
m = 1 \pmod{5}
\]

Backsolve: \( b = 2 \pmod{5} \). Secret is 2.
And the line is...
\[
x + 2 \pmod{5}
\]
Delta Polynomials: Concept.

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

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

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: \((x_1, y_1), (x_2, y_2), \ldots, (x_d, y_d)\). Solve...

\[
a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = y_1 \mod p
\]

\[
a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = y_2 \mod p
\]

\[
a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = y_d \mod p
\]

Subtracting 2nd from 3rd yields:

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

\[
3a_1 + 2a_2 = 1 \mod 5
\]

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

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

\[
a_2 = -(1 + 2 - 6) = -5 \equiv 0 \mod 5
\]

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

Polynomials.

We will work with polynomials with arithmetic modulo \( p \).

Everything has a multiplicative inverse.

Like rationals, reals.

Warning: no calculus, and no order even.

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.

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

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

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

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

\[
3a_1 + 2a_2 = 1 \mod 5
\]

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

Another Construction: Lagrange Interpolation!

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

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

Try \((x-2)(x-3) \mod 5\).

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

So “divide by 2” or multiply by 3.

\[
\Delta_1(x) = (x-2)(x-3) \mod 5
\]

\[
\Delta_2(x) = (x-1)(x-3) \mod 5
\]

\[
\Delta_3(x) = (x-1)(x-2) \mod 5
\]

But wanted to hit \((1,3); (2,4); (3,0)\).

\[
P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)
\]

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 polynomial having degree \( \leq d \) with arithmetic modulo prime \( p \) contains \( d+1 \) pts.

Proof of at least one polynomial:

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

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

Numerator is 0 at \( x_i \neq x_j \).

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

Work modulo 5.
\[ \Delta_1(x) \] contains (1,1) and (3,0).
\[ \Delta(x) = \frac{1 - 3}{2} = \frac{4}{2} = 2x - 6 = 2x + 4 \mod 5. \]
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).
\[ \Delta_1(x) = \frac{1 - 2(x - 3)}{2(x - 3)} = \frac{4}{2} = 2x + 4 \mod 5. \]
Put the delta functions together.

Uniqueness.

Uniqueness Fact. At most one degree \( d \) polynomial hits \( d + 1 \) points.

Proof:
Roots fact: Any degree \( d \) polynomial has at most \( d \) roots.
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.

In general.

Polynomial Division.

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

\[
\begin{array}{r|rrr}
 & 4 & x & + & 4 \\
\hline
 x - 3 & | 4x & 2 & - & 3 \\
 & 4x & 2 & - & 2x \\
 & & 4x & + & 2 \\
 & & 4x & - & 2 \\
 & & & - & 4 \\
\end{array}
\]

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

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

Where have we seen this concept before? (Hint: CRT)

My love is won. Zero and one. Nothing done.

Find \( x = a \mod m \) and \( x = b \mod n \) where \( \gcd(m,n)=1 \).
Solution: \( x = au + bv \), where \( u = 0 \mod n \) and \( u = 1 \mod m \)
\( v = 1 \mod n \) and \( v = 0 \mod m \)

Similar deal here with the Delta polynomials in Lagrange interpolation.

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; \( n_1, \ldots ,n_d \) then
\[ P(x) = \prod_{i=1}^{d} (x-n_i). \]

Proof Sketch: By induction.

Induction Step: \( P(x) = (x-n_k)Q(x) \) 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 \( \mathbb{F}_m \) or \( \text{GF}(m) \).
Intuitively, a field is a set with operations corresponding to addition, multiplication, and division.

History lesson: Evariste Galois (1811-1832)

Modular Arithmetic Fact: There exists exactly one polynomial having degree \( \leq d \) over \( \text{GF}(p) \), \( P(x) \), 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 randomly \( a_1,\ldots,a_{k-1} \).
2. Let \( P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0 \) with \( a_0 = s \).
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.

Secret Sharing

Minimality.
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 \( 2n \).
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.
**Erasure Codes.**

Satellite

3 packet message. So send 6!

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
</table>

Lose 3 out 6 packets.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
</table>

GPS device

Gets packets 1, 1, and 3.

---

**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.

Alright!!!!!!

Use polynomials.

---

**Information Theory.**

Size: Can choose a prime between $2^b - 1$ and $2^b$.

(Lose at most 1 bit per packet.)

But: packets need label for $x$ value.

There are Galois Fields $GF(2^n)$ where one loses nothing.

– Can also run the Fast Fourier Transform.

In practice, $O(n)$ operations with almost the same redundancy.

Comparison with Secret Sharing: information content.

Secret Sharing: each share is size of whole secret.

Coding: Each packet has size $1/n$ of the whole message.

---

**Erasure Code: Example.**

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.

Linear System.

Work modulo 5.

$P(x) = x^2$ (mod 5)

$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4$ (mod 5)

Send $(0, P(0)) \ldots (5, P(5))$.

6 points. Better work modulo 7 at least!

Why? $(0, P(0)) = (5, P(5))$ (mod 5)
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]

6$a_1$ + 3$a_0$ = 2 (mod 7), 5$a_1$ + 4$a_0$ = 0 (mod 7)
\[
a_1 = 2$ a_0$ = 2 (mod 7) a_1 = 4 (mod 7) a_2 = 2 (mod 7)
\]
\[
P(x) = 2x^2 + 4x + 2
\]
$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$
Send
Packets: (1,1), (2,4), (3,4), (4,7), (5,2), (6,0)
Notice that packets contain “x-values”.

Bad reception!

Send: (1,1),(2,4),(3,4),(4,7),(5,2),(6,0)
Recieve: (1,1) (3,4), (6,0)
Reconstruct?
Format: $(i, R(i))$. Lagrange or linear equations.

P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}

Channeling Sahai ...

P(x) = 2x^2 + 4x + 2
Message? $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

Questions for Review

You want to encode a secret consisting of 1,4,4.
How big should modulus be? Larger than 144 and prime!
You want to send a message consisting of packets 1,4,2,3,0 through a noisy channel that loses 3 packets.
How big should modulus be? Larger than 8 and prime!
Send $n$ packets $b$-bit packets, with $k$ errors.
Modulus should be larger than $n + k$ and also larger than $2^b$.

Polynomials.

- ..give Secret Sharing.
- ..give Erasure Codes.

Error Correction:
Noisy Channel: corrupts $k$ packets. (rather than loss.)
Additional Challenge: Finding which packets are corrupt.