Today.
Today.

Polynomials.
Today.

Polynomials.

Secret Sharing.
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.
Secret Sharing.

Share secret among \( n \) people.
Secret Sharing.

Share secret among \( n \) people.

Secrecy: Any \( k - 1 \) knows nothing.
Secret Sharing.

Share secret among $n$ people.

Secrecy: Any $k - 1$ knows nothing.
Roubustness: Any $k$ knows secret.
Secret Sharing.

Share secret among \( n \) people.

Secrecy: Any \( k - 1 \) knows nothing.

Robustness: Any \( k \) knows secret.

Efficient: minimize storage.
Share secret among \( n \) people.

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

**Roubustness:** Any \( k \) knows secret.

**Efficient:** minimize storage.
Secret Sharing.

Share secret among \( n \) people.

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

**Roubustness:** Any \( k \) knows secret.

**Efficient:** minimize storage.

The idea of the day.
Share secret among $n$ people.

**Secrecy:** Any $k - 1$ knows nothing.

**Robustness:** Any $k$ knows secret.

**Efficient:** minimize storage.

The idea of the day.
Secret Sharing.

Share secret among \( n \) people.

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

**Roubustness:** Any \( k \) knows secret.

**Efficient:** minimize storage.

The idea of the day.

  Two points make a line.
Secret Sharing.

Share secret among $n$ people.

**Secrecy:** Any $k - 1$ knows nothing.

**Roubustness:** 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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

\( P(x) \) **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** \( p \): ¹ \( a_i \in \{0, \ldots, p-1\} \)
and

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

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

¹A field is a set of elements with addition and multiplication operations, with inverses. \( GF(p) = (\{0, \ldots, p-1\}, + \pmod{p}, \cdot \pmod{p}) \).
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

Line: \( P(x) = a_1 x + a_0 \)
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

Line: \( P(x) = a_1 x + a_0 = mx + b \)
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

Line: \( P(x) = a_1 x + a_0 = mx + b \)
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

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

\[ P(x) = .5x + 0 \]
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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

Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

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

Parabola: \( P(x) = a_2 x^2 + a_1 x + a_0 \)
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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

Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

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

Parabola: \( P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c \)
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \)

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

Parabola: \( P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c \)
Polynomial: \( P(x) = a_d x^4 + \cdots + a_0 \pmod{p} \)

Finding an intersection.

\[ x + 2 \equiv 3 x + 1 \pmod{5} \]

\[ \Rightarrow 2 x \equiv 1 \pmod{5} \]

\[ \Rightarrow x \equiv 3 \pmod{5} \]

3 is multiplicative inverse of 2 modulo 5.

Good when modulus is prime!!
Polynomial: $P(x) = a_d x^4 + \cdots + a_0 \pmod{p}$

Finding an intersection:

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

3 is multiplicative inverse of 2 modulo 5.

Good when modulus is prime!!
Polynomial: $P(x) = a_d x^4 + \cdots + a_0 \pmod{p}$

Finding an intersection.

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

$\implies 2x \equiv 1 \pmod{5}$
Polynomial: \( P(x) = a_dx^4 + \cdots + a_0 \pmod{p} \)

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

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.  

\[ ^2 \text{Points with different } x \text{ values.} \]
Two points make a line.

**Fact:** Exactly 1 degree $\leq d$ polynomial contains $d + 1$ points. \(^2\)

Two points specify a line.

\(^2\)Points with different $x$ values.
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.

---

$^2$Points with different $x$ values.
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.

\(^2\)Points with different $x$ values.
Two points determine a line. What facts below tell you this?

Say points are \((x_1, y_1), (x_2, y_2)\).
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.
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.
Why solution? Why unique?

(A) Solution cuz:
\[
m = \frac{y_2 - y_1}{x_2 - x_1},
\]
\[
b = y_1 - m(x_1).
\]

(B) Unique cuz, only one line goes through two points.

(C) Try:
\[
(m'x + b') - (mx + b) = m'x + b' - mx - b = ax + c \neq 0.
\]

(D) Either
\[
a x_1 + c \neq 0 \text{ or } a x_2 + c \neq 0.
\]

(E) Contradiction.

Flow Poll. (All true. (B) is not a proof, it is restatement.)
Why solution? Why unique?

(A) Solution cuz: \( m = \frac{y_2 - y_1}{x_2 - x_1}, \ b = y_1 - m(x_1) \)

(B) Unique cuz, only one line goes through two points.

(C) Try: \( (m'x + b') - (mx + b) = (m' - m)x + (b - b') = ax + c \neq 0 \).

(D) Either \( ax_1 + c \neq 0 \) or \( ax_2 + c \neq 0 \).

(E) Contradiction.
Why solution? Why unique?

(A) Solution cuz: \( m = \frac{y_2 - y_1}{x_2 - x_1} \), \( b = y_1 - m(x_1) \)

(B) Unique cuz, only one line goes through two points.

(C) Try: \((m'x + b') - (mx + b) = (m' - m)x + (b - b') = ax + c \neq 0\).

(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: $a_n x^n + \cdots + a_0$. 
Notation: two points on a line.

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

Consider line: $mx + b$
Notation: two points on a line.

Polynomial: \( a_n x^n + \cdots + a_0 \).

Consider line: \( mx + b \)

(A) \( a_1 = m \)
(B) \( a_1 = b \)
(C) \( a_0 = m \)
(D) \( a_0 = b \).
Notation: two points on a line.

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

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. $^3$
3 points determine a parabola.

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

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

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

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

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

Fact: Exactly 1 degree $\leq d$ polynomial contains $d + 1$ points.
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 determine a parabola.

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

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

\[ P(x) = -0.3x^2 + 1x + 0.5 \]

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

\(^3\)Points with different \( x \) values.
2 points not enough.

There is $P(x)$ contains blue points and *any* $(0, y)$!
There is $P(x)$ contains blue points and any $(0, y)$!
2 points not enough.

There is $P(x)$ contains blue points and any $(0, y)$!
There is $P(x)$ contains blue points and any $(0, y)$!
2 points not enough.

There is $P(x)$ contains blue points and any $(0, y)!$
There is $P(x)$ contains blue points and any $(0, y)$!
2 points not enough.

There is $P(x)$ contains blue points and any $(0, y)$!
2 points not enough.

There is $P(x)$ contains blue points and *any* $(0, y)$!
2 points not enough.

\[ P(x) = 0.2x^2 - 0.5x + 1.5 \]

\[ P(x) = -0.3x^2 + 1x + 0.5 \]

\[ P(x) = -0.6x^2 + 1.9x - 0.1 \]
2 points not enough.

$P(x) = 0.2x^2 - 0.5x + 1.5$

$P(x) = -0.3x^2 + 1.0x + 0.5$

$P(x) = -0.6x^2 + 1.9x - 0.1$

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:
Secrets \( s \in \{0, \ldots, p-1\} \)

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
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 \( k \) shares gives secret.
Knowing \( k \) pts \( \Rightarrow \) only one \( P(x) \Rightarrow \) evaluate \( P(0) \).

Secrecy: Any \( k - 1 \) shares give nothing.
Knowing \( \leq k - 1 \) pts \( \Rightarrow \) any \( P(0) \) is possible.
Modular Arithmetic Fact and Secrets

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

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 $k$ shares gives secret.

**Secrecy:** Any $k-1$ shares give nothing.
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 \( s \in \{0, \ldots, p - 1\} \)
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 $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$. 
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 \( s \in \{0, \ldots, p - 1\} \)

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
2. Let \( P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0 \) with \( a_0 = s \).
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 $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 $k$ shares gives secret. Knowing $k$ pts $\Rightarrow$ only one $P(x) \Rightarrow$ evaluate $P(0)$.

Secrecy: Any $k-1$ shares give nothing. Knowing $\leq k-1$ pts $\Rightarrow$ any $P(0)$ is possible.
**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 $s \in \{0, \ldots, p-1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 $(i, P(i) \mod p)$.

**Roublteness:** Any $k$ shares gives secret.
Knowing $k$ pts $\Rightarrow$ only one $P(x)$ $\Rightarrow$ evaluate $P(0)$.

**Secrecy:** Any $k-1$ shares give nothing.
Knowing $\leq k-1$ pts $\Rightarrow$ any $P(0)$ is possible.
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 \( s \in \{0, \ldots, p-1\} \)

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

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

**Secrecy:** Any \( k-1 \) shares give nothing. Knowing \( \leq k-1 \) pts \( \Rightarrow \) any \( P(0) \) is possible.
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 \( s \in \{0, \ldots, p - 1\} \)

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
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 \((i, P(i) \mod p)\).

**Roubustness:** Any \( k \) shares gives secret.
Knowing \( k \) pts
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 $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 $k$ shares gives secret.
Knowing $k$ pts $\implies$ only one $P(x)$
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 \( s \in \{0, \ldots, p-1\} \)

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
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 \( k \) shares gives secret.
Knowing \( k \) pts \( \implies \) only one \( P(x) \implies \) evaluate \( P(0) \).
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 $s \in \{0, \ldots, p-1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 $(i, P(i) \mod p)$.

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.
**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 \( s \in \{0, \ldots, p - 1\} \)

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
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 \((i, P(i) \mod p)\).

**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
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 \( s \in \{0, \ldots, p-1\} \)

1. Choose \( a_0 = s \), and random \( a_1, \ldots, a_{k-1} \).
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 \( k \) 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.
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 $s \in \{0, \ldots, p-1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 $(i, P(i) \mod p)$.

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.
The polynomial from the scheme: $P(x) = 2x^2 + 1x + 3 \pmod{5}$. What is true for the secret sharing scheme using $P(x)$?
The polynomial from the scheme: \( P(x) = 2x^2 + 1x + 3 \pmod{5} \). What is true for the secret sharing scheme using \( P(x) \)?

(A) The secret is “2”.
(B) The secret is “3”.
(C) A share could be \((1, 5)\) cuz \( P(1) = 5 \)
(D) A share could be \((2, 4)\)
(E) A share could be \((0, 3)\)
From $d + 1$ points to degree $d$ polynomial?

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

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 $x + 2 \pmod{5}$. 
From $d + 1$ points to degree $d$ polynomial?

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

\[ P(1) = \]

\[ P(2) = \]

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...

\[ x + 2 \pmod{5} \]
From $d + 1$ points to degree $d$ polynomial?

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

$P(1) = m(1) + b \equiv m + b$
From $d + 1$ points to degree $d$ polynomial?

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

$$P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}$$
From $d + 1$ points to degree $d$ polynomial?

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

\[
P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}
\]
\[
P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5}
\]
From $d + 1$ points to degree $d$ polynomial?

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

\[
P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}
\]
\[
P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5}
\]
From $d + 1$ points to degree $d$ polynomial?

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

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

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

Subtract first from second..
From $d + 1$ points to degree $d$ polynomial?

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

\[ P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5} \]
\[ P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5} \]

Subtract first from second..

\[ m + b \equiv 3 \pmod{5} \]
\[ m \equiv 1 \pmod{5} \]

Secret is 2.

And the line is...

$x + 2 \pmod{5}$. 
From $d + 1$ points to degree $d$ polynomial?

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

\[
P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}
\]
\[
P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5}
\]

Subtract first from second..

\[
m + b \equiv 3 \pmod{5}
\]
\[
m \equiv 1 \pmod{5}
\]

Backsolve: $b \equiv 2 \pmod{5}$. 
From $d + 1$ points to degree $d$ polynomial?

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

\[
P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}
\]
\[
P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5}
\]

Subtract first from second..

\[
m + b \equiv 3 \pmod{5}
\]
\[
m \equiv 1 \pmod{5}
\]

Backsolve: $b \equiv 2 \pmod{5}$. Secret is 2.
From $d + 1$ points to degree $d$ polynomial?

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

\[
P(1) = m(1) + b \equiv m + b \equiv 3 \pmod{5}
\]
\[
P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod{5}
\]

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...

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

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

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

$P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}$

Subtracting the 2nd from the 3rd yields:

$a_1 = 1$.

$a_0 = (2 - 4(1)) \equiv 1 \pmod{5}$

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

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

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

$$P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}$$
$$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}$$
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.

\[ P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5} \]
\[ P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5} \]
\[ P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5} \]
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.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]
For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1, 2); (2, 4); (3, 0)$. Plug in points to find equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]

\[
a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
3a_1 + 2a_0 \equiv 1 \pmod{5}
\]
\[
4a_1 + 2a_0 \equiv 2 \pmod{5}
\]
For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1, 2); (2, 4); (3, 0)$. Plug in points to find equations.

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

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

$P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}$

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

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

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

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

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

\[
\begin{align*}
a_2 + a_1 + a_0 &\equiv 2 \pmod{5} \\
3a_1 + 2a_0 &\equiv 1 \pmod{5} \\
4a_1 + 2a_0 &\equiv 2 \pmod{5}
\end{align*}
\]

Subtracting 2nd from 3rd yields: \( a_1 = 1 \).
\[
a_0 = (2 - 4(a_1))2^{-1}
\]
For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2); (2,4); (3,0)$. Plug in points to find equations.

\begin{align*}
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) &= 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\end{align*}

\begin{align*}
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}
\end{align*}

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

$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1})$
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.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]

\[
a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
3a_1 + 2a_0 \equiv 1 \pmod{5}
\]
\[
4a_1 + 2a_0 \equiv 2 \pmod{5}
\]

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

$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3)$
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.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]

\[
a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
3a_1 + 2a_0 \equiv 1 \pmod{5}
\]
\[
4a_1 + 2a_0 \equiv 2 \pmod{5}
\]

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

\[
a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod{5}
\]
For a quadratic polynomial, \( a_2x^2 + a_1x + a_0 \) hits \((1,2);(2,4);(3,0)\). Plug in points to find equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]

\[
a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
3a_1 + 2a_0 \equiv 1 \pmod{5}
\]
\[
4a_1 + 2a_0 \equiv 2 \pmod{5}
\]

Subtracting 2nd from 3rd yields: \( a_1 = 1 \).
\[
a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod{5}
\]
\[
a_2 = 2 - 1 - 4 \equiv 2 \pmod{5}
\]
For a quadratic polynomial, \( a_2x^2 + a_1x + a_0 \) hits \((1,2); (2,4); (3,0)\).
Plug in points to find equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]

\[
a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
3a_1 + 2a_0 \equiv 1 \pmod{5}
\]
\[
4a_1 + 2a_0 \equiv 2 \pmod{5}
\]

Subtracting 2nd from 3rd yields: \( a_1 = 1 \).
\[
a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod{5}
\]
\[
a_2 = 2 - 1 - 4 \equiv 2 \pmod{5}.
\]
For a quadratic polynomial, \( a_2x^2 + a_1x + a_0 \) hits \( (1,2); (2,4); (3,0) \). Plug in points to find equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{5}
\]
\[
P(3) = 4a_2 + 3a_1 + a_0 \equiv 0 \pmod{5}
\]

\[
a_2 + a_1 + a_0 \equiv 2 \pmod{5}
\]
\[
3a_1 + 2a_0 \equiv 1 \pmod{5}
\]
\[
4a_1 + 2a_0 \equiv 2 \pmod{5}
\]

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: \((x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)\).
In general..

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

Solve...

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

Will this always work?

As long as solution exists and it is unique!

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

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

Solve...

\[ a_{k-1}x_1^{k-1} + \cdots + a_0 \equiv y_1 \pmod{p} \]
\[ a_{k-1}x_2^{k-1} + \cdots + a_0 \equiv y_2 \pmod{p} \]
\[ \cdots \]
\[ a_{k-1}x_k^{k-1} + \cdots + a_0 \equiv y_k \pmod{p} \]

Will this always work?
In general..

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

Solve...

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

Will this always work?

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

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

Solve...

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

Will this always work?

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

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

Solve...

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

Will this always work?

As long as solution \textbf{exists} and it is \textbf{unique}! And...

\textbf{Modular Arithmetic Fact:} Exactly 1 degree \(\leq d\) polynomial with arithmetic modulo prime \(p\) contains \(d + 1\) pts.
Another Construction: Interpolation!

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

For a quadratic, $a_2 x^2 + a_1 x + a_0$ hits $(1, 2); (2, 4); (3, 0)$.
Find $\Delta_1(x)$ polynomial contains $(1, 1); (2, 0); (3, 0)$.
Another Construction: Interpolation!

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

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

Try \((x - 2)(x - 3) \pmod{5}\).
Another Construction: Interpolation!

For a quadratic, $a_2 x^2 + a_1 x + a_0$ hits $(1, 2); (2, 4); (3, 0)$. 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.
Another Construction: Interpolation!

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

For a quadratic, $a_2 x^2 + a_1 x + a_0$ hits $(1,2); (2,4); (3,0)$.
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!!
Another Construction: Interpolation!

For a quadratic, \( a_2 x^2 + a_1 x + a_0 \) hits \((1, 2); (2, 4); (3, 0)\).
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.
\[ \Delta_1(x) = (x - 2)(x - 3)(3) \pmod{5} \]
Another Construction: Interpolation!

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

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 $(1, 1); (2, 0); (3, 0)$. 
Another Construction: Interpolation!

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

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 \((1, 0); (2, 1); (3, 0)\).
Another Construction: Interpolation!

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

$P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?...after a lot of calculations...

$P(x) = 2x^2 + 1x + 4 \pmod{5}$. 

The same as before!
Another Construction: Interpolation!

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

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

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 $(1, 2); (2, 4); (3, 0)$!

$P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.
Another Construction: Interpolation!

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

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 $(1, 2); (2, 4); (3, 0)$!

$P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?
Another Construction: Interpolation!

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

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 \((1,2); (2,4); (3,0)\)!

\( P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x) \) works.

Same as before?

...after a lot of calculations...
Another Construction: Interpolation!

For a quadratic, \(a_2 x^2 + a_1 x + a_0\) hits \((1, 2); (2, 4); (3, 0)\).
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 \((1, 2); (2, 4); (3, 0)!\)
\(P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)\) works.
Same as before?
...after a lot of calculations... \(P(x) = 2 x^2 + 1 x + 4 \pmod{5}\).
Another Construction: Interpolation!

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

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.

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

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

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

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

\[
P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x) \text{ works.}
\]

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 $x \in \{1, \ldots, p-1\}$.
Flowers, and grass, oh so nice.
Fields...

Flowers, and grass, oh so nice.

Set and two commutative operations: addition and multiplication with additive/multiplicative identities and inverses expect 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 $\gcd(x, p) = 1$, forall $x \in \{1, \ldots, p-1\}$. 
Flowers, and grass, oh so nice.

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

E.g., Reals, rationals, complex numbers.
Flowers, and grass, oh so nice.

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

E.g., Reals, rationals, complex numbers.
Not E.g., the integers, matrices.
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.
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 $p$. 
Flowers, and grass, oh so nice.

Set and two commutative operations: addition and multiplication with additive/multiplicative identities and inverses expect 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.
Flowers, and grass, oh so nice.

Set and two commutative operations: addition and multiplication with additive/multiplicative identities and inverses expect 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).
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 \( \gcd(x, p) = 1 \), forall \( x \in \{1, \ldots, p - 1\} \)
Delta Polynomials: Concept.

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

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

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

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

\[
\Delta_i(x) = \begin{cases} 
1, & \text{if } x = x_i. \\
0, & \text{if } x = x_j \text{ for } j \neq i. \\
?, & \text{otherwise.}
\end{cases}
\] (1)
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?
Delta Polynomials: Concept.

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

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

(1)

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

See the idea? Function that contains all points?

$$P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + \ldots + y_{d+1} \Delta_{d+1}(x).$$
Delta Polynomials: Concept.

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

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

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 $(x_1, y_1)$?
Delta Polynomials: Concept.

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

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

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 $(x_2, y_2)$?
Delta Polynomials: Concept.

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

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

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

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

(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 \((x_1, y_1)\)?
Delta Polynomials: Concept.

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

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

(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 $(x_2, y_2)$?
Delta Polynomials: Concept.

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

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

$$\text{(1)}$$

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?
Delta Polynomials: Concept.

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

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

(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?
Delta Polynomials: Concept.

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

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

(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?

\[
P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x)
\]
Delta Polynomials: Concept.

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

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

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?

$$P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) \ldots + y_{d+1} \Delta_{d+1}(x).$$
There exists a polynomial...
There exists a polynomial...

**Modular Arithmetic Fact:** Exactly 1 degree ≤ $d$ polynomial with arithmetic modulo prime $p$ contains $d + 1$ pts.
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: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$. 
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: \((x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})\).

\[
\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}
\]
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: \((x_1, y_1);(x_2, y_2) \cdots (x_{d+1}, y_{d+1})\).

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

\[
P(x) = y_1\Delta_1(x) + y_2\Delta_2(x) + \cdots + y_{d+1}\Delta_{d+1}(x).
\]
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 \((x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})\).
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!
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!
Mark what’s true.
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) $\Delta_2(x_2) = 1$
(F) $\Delta_2(x_1) = 0$
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) $\Delta_2(x_2) = 1$
(F) $\Delta_2(x_1) = 0$

(B), (C), and (E)
Example.

\[ \Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}. \]
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 \((3,4)\)?
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.
Example.

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

Degree 1 polynomial, \( P(x) \), that contains \((1,3)\) and \((3,4)\)?
Work modulo 5.
\( \Delta_1(x) \) contains \((1,1)\) and \((3,0)\).
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).
\[ \Delta_1(x) = \frac{(x - 3)}{1 - 3} = \frac{x - 3}{-2} = (x - 3)(-2)^{-1} \]
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).

\[ \Delta_1(x) = \frac{(x-3)}{1-3} = \frac{x-3}{-2} = (x - 3)(-2)^{-1} \]
\[ \Delta_1(x) = (x - 3)(1 - 3)^{-1} = (x - 3)(-2)^{-1} \]
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 \((3, 0)\).

\[ \Delta_1(x) = \frac{(x-3)}{1-3} = \frac{x-3}{-2} = (x - 3)(-2)^{-1} \]
\[ \Delta_1(x) = (x - 3)(1 - 3)^{-1} = (x - 3)(-2)^{-1} \]
\[ = 2(x - 3) \]
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 \((3,0)\).

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

\[
\Delta_1(x) = (x - 3)(1 - 3)^{-1} = (x - 3)(-2)^{-1}
\]

\[
= 2(x - 3) = 2x - 6
\]
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 \( (3,0) \).

\[ \Delta_1(x) = \frac{(x-3)}{1-3} = \frac{x-3}{-2} = (x-3)(-2)^{-1} \]
\[ \Delta_1(x) = (x-3)(1-3)^{-1} = (x-3)(-2)^{-1} \]
\[ = 2(x-3) = 2x - 6 = 2x + 4 \pmod{5}. \]
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 \((3,0)\).

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

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

\[ \Delta_1(x) = \frac{(x-3)}{1-3} = \frac{x-3}{-2} = (x - 3)(-2)^{-1} \]
\[ \Delta_1(x) = (x - 3)(1 - 3)^{-1} = (x - 3)(-2)^{-1} \]
\[ \quad = 2(x - 3) = 2x - 6 = 2x + 4 \pmod 5. \]

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

Work modulo 5.
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 $(3,0)$.

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

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

Put the delta functions together.
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.

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

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

\[ \Delta_1(x) = (x - 3)(1 - 3)^{-1} = (x - 3)(-2)^{-1} \]

\[ = 2(x - 3) = 2x - 6 = 2x + 4 \pmod{5}. \]

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).

\[ \Delta_1(x) = \frac{(x - 2)(x - 3)}{(1 - 2)(1 - 3)} \]
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).

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

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).

\[ \Delta_1(x) = \frac{(x - 2)(x - 3)}{(1 - 2)(1 - 3)} = \frac{(x - 2)(x - 3)}{2} \]
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 \((3,0)\).

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

\[
\Delta_1(x) = (x-3)(1-3)^{-1} = (x-3)(-2)^{-1}
\]

\[
= 2(x-3) = 2x-6 = 2x+4 \pmod{5}.
\]

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

\[
\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = (2)^{-1}(x-2)(x-3)
\]
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 $(3,0)$.

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

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

$$= 2(x-3) = 2x - 6 = 2x + 4 \pmod{5}.$$ 

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

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = (2)^{-1}(x-2)(x-3) = 3(x-2)(x-3)$$
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 \((3,0)\).

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

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

\[ \Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = (2)^{-1}(x - 2)(x - 3) = 3(x - 2)(x - 3) \]
\[ = 3x^2 + 3 \pmod{5} \]
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 \((3, 0)\).

\[
\begin{align*}
\Delta_1(x) &= \frac{(x-3)}{1-3} = \frac{x-3}{-2} = (x - 3)(-2)^{-1} \\
\Delta_1(x) &= (x - 3)(1 - 3)^{-1} = (x - 3)(-2)^{-1} \\
&= 2(x - 3) = 2x - 6 = 2x + 4 \pmod{5}.
\end{align*}
\]

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

\[
\begin{align*}
\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = (2)^{-1}(x - 2)(x - 3) = 3(x - 2)(x - 3) \\
&= 3x^2 + 3 \pmod{5}.
\end{align*}
\]
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 $(3,0)$.

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

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

$$= 2(x-3) = 2x - 6 = 2x + 4 \; (\text{mod } 5).$$

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

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

$$= 3x^2 + 3 \; (\text{mod } 5)$$

Put the delta functions together.
In general.

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

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

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

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

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

The numerator is 0 at \(x_j \neq x_i\).

The 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!
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 \(x_j \neq x_i\).
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 \(x_i\).
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 \((x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)\).
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.
Uniqueness.

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

Roots fact: Any nontrivial degree $d$ polynomial has at most $d$ roots.
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 $x$. 
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.
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.
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 $d$. 
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.
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.
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.
Polynomial Division.

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

\[
\begin{array}{c|cc}
\text{x} & 4 & x \\
\hline
x - 3 & 4x^2 & -3x + 2 \\
\end{array}
\]

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

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

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

\[
\begin{array}{c}
4x \\
\hline
x - 3 \mid 4x^2 - 3x + 2 \\
\hline
4x^2 - 2x \\
\hline
4x + 2 \\
\hline
4x - 2 \\
\hline
4
\end{array}
\]

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

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

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

$$
\begin{array}{c}
  4x + 4 \\
  \hline \\
  x - 3 | 4x^2 - 3x + 2 \\
  - (4x^2 - 2x) \\
  \hline \\
  4x + 2
\end{array}
$$

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

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

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

\[
\begin{array}{r}
4x & + & 4 \\
\hline
x - 3 & ) & 4x^2 & - & 3x & + & 2 \\
& & 4x^2 & - & 2x \\
\hline
& & 4x & + & 2 \\
& & 4x & - & 2
\end{array}
\]
Polynomial Division.

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

\[
\begin{array}{c|ccccc}
& 4x & + & 4 \\
\hline
x - 3 & ) 4x^2 & - & 3x & + & 2 \\
& 4x^2 & - & 2x & & \\
\hline
& 4x & + & 2 \\
& 4x & - & 2 & & \\
\hline
& 4
\end{array}
\]

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

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

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

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

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

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

\[
\begin{array}{cccc}
\text{x} & \text{+} & \text{x} & \text{+} & \text{4} & \text{r} & \text{4} \\
\hline
\text{x} & \text{-} & \text{3} & \text{)} & \text{4x}^2 & \text{-} & \text{3x} & \text{+} & \text{2} \\
\text{4x}^2 & \text{-} & \text{2x} & \hline
\text{4x} & \text{+} & \text{2} \\
\text{4x} & \text{-} & \text{2} & \hline
\text{4} \\
\end{array}
\]

\[4x^2 - 3x + 2 \equiv (x - 3)(4x + 4) + 4 \pmod{5}\]
Polynomial Division.

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

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

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

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

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

\[
\begin{array}{cccc}
4 & x & + & 4 & r & 4 \\
\hline
x & - & 3 & ) & 4x^2 & - & 3x & + & 2 \\
4x^2 & - & 2x & & & & & & \\
\hline & & 4x & + & 2 \\
4x & - & 2 & & & & & & \\
\hline & & & 4 \\
\end{array}
\]

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

In general, divide $P(x)$ by $(x - a)$ gives $Q(x)$ and remainder $r$. That is, $P(x) = (x - a)Q(x) + r$
Lemma 1: $P(x)$ has root $a$ iff $P(x)/(x - a)$ has remainder 0: $P(x) = (x - a)Q(x)$. 

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

---

**Lemma 2:** $P(x)$ has $d$ roots; $r_1, ..., r_d$ 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.
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 $r = 0$. 
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 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 $P(x) = c(x - r_1)(x - r_2) \cdots (x - r_d)$. 

Only $d$ roots.
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.
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: $P(x) = (x - r_1)Q(x)$ by Lemma 1. $Q(x)$ has smaller
degree so use the induction hypothesis.
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: \( P(x) = (x - r_1)Q(x) \) by Lemma 1. \( Q(x) \) has smaller degree so use the induction hypothesis.
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: \( P(x) = (x - r_1)Q(x) \) by Lemma 1. \( Q(x) \) has smaller degree so use the induction hypothesis.

\( d + 1 \) roots implies degree is at least \( d + 1. \)
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: $P(x) = (x - r_1)Q(x)$ 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.
Proof works for reals, rationals, and complex numbers.
Proof works for reals, rationals, and complex numbers.

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

Finite Fields
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..
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.
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.
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 $GF(m)$.  

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.
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 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 $s \in \{0, \ldots, p - 1\}$
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 \( s \in \{0, \ldots, p - 1\} \)

1. Choose \( a_0 = s \), and randomly \( a_1, \ldots, a_{k-1} \).
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 $s \in \{0, \ldots, p-1\}$

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 $a_0 = s$. 

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

**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 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 $(i, P(i) \mod p)$.
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 $s \in \{0, \ldots, p-1\}$

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 $(i, P(i) \mod p)$.
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 \( s \in \{0, \ldots, p - 1\} \)

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.
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 $s \in \{0, \ldots, p - 1\}$

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

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

**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 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.
Minimality.

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

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$. For $b$-bit secret, must choose a prime $p > 2^b$. 
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,*
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,*
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*
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 $2n$.*
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.**
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, \( P(x) \).
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 \( P(0) \)!
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!
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.

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.
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 $GF(m)$?
A bit more counting.

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

- $m^{d+1}$: $d + 1$ coefficients from $\{0, \ldots, m-1\}$. 

Infinite number for reals, rationals, complex numbers!
A bit more 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 $\{0, \ldots, m-1\}$.
A bit more 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!
Summary

Two points make a line.
Summary

Two points make a line.

Compute solution: $m, b$. 
Summary

Two points make a line.

Compute solution: $m, b$.
Unique:
Summary

Two points make a line.

Compute solution: \( m, b \).

Unique:

Assume two solutions, show they are the same.
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.
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.
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.
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 $d$. 
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.
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 \( \implies P(x) = Q(x) \).
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.