Lecture 14. Outline.

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

Modular Arithmetic Fact and Secrets

Modular Arithmetic Fact and Secrets

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

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
Secret $s \in \{0, \ldots, p-1\}$

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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: There is exactly 1 polynomial of degree $\leq d$ with arithmetic modulo prime p that contains $d+1$ pts.

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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: There is exactly 1 polynomial of degree $\leq d$ with arithmetic modulo prime p that contains $d+1$ pts.

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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 $(i, P(i) \mod p)$.

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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.

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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.

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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, find unique $P(x)$, evaluate $P(0)$.

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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, find unique $P(x)$, evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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, find unique $P(x)$, evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.

Modular Arithmetic Fact and Secrets

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

Note: The points have to have different x values!

Shamir's k out of n Scheme:
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, find unique $P(x)$, evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.
Knowing $\leq k-1$ pts, any $P(0)$ is possible.

There exists a polynomial...

There exists a polynomial...

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ 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: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

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

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

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

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

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

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

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

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

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

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

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!

Reiterating Examples.

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

Reiterating Examples.

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

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

Reiterating Examples.

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

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

Work modulo 5.

Reiterating Examples.

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

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

Work modulo 5.

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

$$\begin{aligned}\Delta_1(x) &= \frac{(x-3)}{1-3} = \frac{x-3}{-2} \\ &= 2(x-3)\end{aligned}$$

Reiterating Examples.

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

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

Work modulo 5.

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

$$\begin{aligned}\Delta_1(x) &= \frac{(x-3)}{1-3} = \frac{x-3}{-2} \\ &= 2(x-3) = 2x-6\end{aligned}$$

Reiterating Examples.

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

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

Work modulo 5.

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

Work modulo 5.

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

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

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

$$\begin{aligned}\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = 3(x-2)(x-3) \\ &= 3x^2+1 \pmod 5\end{aligned}$$

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

$$\begin{aligned}\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = 3(x-2)(x-3) \\ &= 3x^2+1 \pmod 5\end{aligned}$$

Reiterating Examples.

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

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

Work modulo 5.

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

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

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

$$\begin{aligned}\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = 3(x-2)(x-3) \\ &= 3x^2+1 \pmod 5\end{aligned}$$

Put the delta functions together.

Simultaneous Equations Method.

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

Simultaneous Equations Method.

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

$$P(1) =$$

Simultaneous Equations Method.

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

$$P(1) = m(1) + b \quad \equiv \quad m + b$$

Simultaneous Equations Method.

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

$$P(1) = m(1) + b \quad \equiv \quad m + b \equiv 3 \pmod 5$$

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Subtract first from second..

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Subtract first from second..

$$\begin{aligned} m + b &\equiv 3 \pmod 5 \\ m &\equiv 1 \pmod 5 \end{aligned}$$

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Subtract first from second..

$$\begin{aligned} m + b &\equiv 3 \pmod 5 \\ m &\equiv 1 \pmod 5 \end{aligned}$$

Backsolve: $b \equiv 2 \pmod 5$.

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Subtract first from second..

$$\begin{aligned} m + b &\equiv 3 \pmod 5 \\ m &\equiv 1 \pmod 5 \end{aligned}$$

Backsolve: $b \equiv 2 \pmod 5$. Secret is 2.

Simultaneous Equations Method.

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

$$\begin{aligned} P(1) = m(1) + b &\equiv m + b \equiv 3 \pmod 5 \\ P(2) = m(2) + b &\equiv 2m + b \equiv 4 \pmod 5 \end{aligned}$$

Subtract first from second..

$$\begin{aligned} m + b &\equiv 3 \pmod 5 \\ m &\equiv 1 \pmod 5 \end{aligned}$$

Backsolve: $b \equiv 2 \pmod 5$. Secret is 2.

And the line is...

$$x + 2 \mod 5.$$

Quadratic

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

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

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

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2); (2,4); (3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \end{aligned}$$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$. Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$. Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

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

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1}$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1})$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3)$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod 5$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod 5$
$a_2 = 2 - 1 - 4 \equiv 2 \pmod 5$

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod 5$
$a_2 = 2 - 1 - 4 \equiv 2 \pmod 5$.

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.
Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

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...

$$
\begin{aligned}
a_{k-1}x_1^{k-1} + \cdots + a_0 &\equiv y_1 \pmod{p} \\
a_{k-1}x_2^{k-1} + \cdots + a_0 &\equiv y_2 \pmod{p} \\
\vdots \qquad\qquad &\quad \vdots \qquad \vdots \\
a_{k-1}x_k^{k-1} + \cdots + a_0 &\equiv y_k \pmod{p}
\end{aligned}
$$

In general..

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

Solve...

$$
\begin{aligned}
a_{k-1}x_1^{k-1} + \cdots + a_0 &\equiv y_1 \pmod{p} \\
a_{k-1}x_2^{k-1} + \cdots + a_0 &\equiv y_2 \pmod{p} \\
\vdots \qquad\qquad &\quad \vdots \qquad \vdots \\
a_{k-1}x_k^{k-1} + \cdots + a_0 &\equiv y_k \pmod{p}
\end{aligned}
$$

Will this always work?

In general..

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

Solve...

$$\begin{aligned} a_{k-1}x_1^{k-1} + \cdots + a_0 &\equiv y_1 \pmod{p} \\ a_{k-1}x_2^{k-1} + \cdots + a_0 &\equiv y_2 \pmod{p} \\ \vdots \qquad\qquad &\vdots \qquad \vdots \\ a_{k-1}x_k^{k-1} + \cdots + a_0 &\equiv y_k \pmod{p} \end{aligned}$$

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...

$$\begin{aligned} a_{k-1}x_1^{k-1} + \cdots + a_0 &\equiv y_1 \pmod{p} \\ a_{k-1}x_2^{k-1} + \cdots + a_0 &\equiv y_2 \pmod{p} \\ \vdots \qquad\qquad &\vdots \qquad \vdots \\ a_{k-1}x_k^{k-1} + \cdots + a_0 &\equiv y_k \pmod{p} \end{aligned}$$

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...

$$
\begin{aligned}
a_{k-1}x_1^{k-1} + \cdots + a_0 &\equiv y_1 \pmod{p} \\
a_{k-1}x_2^{k-1} + \cdots + a_0 &\equiv y_2 \pmod{p} \\
\vdots \qquad\qquad &\quad \vdots \qquad \vdots \\
a_{k-1}x_k^{k-1} + \cdots + a_0 &\equiv y_k \pmod{p}
\end{aligned}
$$

Will this always work?

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

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

Uniqueness.

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

Uniqueness.

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

Existence: Lagrange interpolation.

Uniqueness.

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

Existence: Lagrange interpolation. Uniqueness?

Uniqueness.

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

Existence: Lagrange interpolation. Uniqueness?

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

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

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

Proof:

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

Proof:

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

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

Proof:

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

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

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

Proof:

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

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

$R(x) = Q(x) - P(x)$ has $d+1$ roots and is degree d.

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

Proof:

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

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

$R(x) = Q(x) - P(x)$ has $d+1$ roots and is degree d.
Contradiction.

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

Proof:

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

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

$R(x) = Q(x) - P(x)$ has $d+1$ roots and is degree d.
Contradiction. $\square$

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

Proof:

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

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

$R(x) = Q(x) - P(x)$ has $d+1$ roots and is degree d.
Contradiction. $\square$
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.

```
                4 x
          -----------------
x - 3 ) 4x^2 - 3 x + 2
```

Polynomial Division.

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

```
                 4 x
          -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
```

Polynomial Division.

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

```
                 4 x + 4
        -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
```

Polynomial Division.

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

```
                 4 x + 4
        -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
```

Polynomial Division.

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

```
                 4 x + 4
        -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

Polynomial Division.

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

```
                 4 x + 4 r 4
        -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

Polynomial Division.

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

```
                 4 x + 4 r 4
          -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

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

Polynomial Division.

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

```
                  4 x + 4 r 4
          -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

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

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.

```
                 4 x + 4 r 4
          -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

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

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

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

Polynomial Division.

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

```
                  4 x + 4 r 4
          -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

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

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

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

r is degree 0 polynomial..

Polynomial Division.

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

```
                  4 x + 4 r 4
          -----------------
x - 3 ) 4x^2 - 3 x + 2
        4x^2 - 2x
        ----------
                 4x + 2
                 4x - 2
                 -------
                      4
```

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

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

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

r is degree 0 polynomial..or a constant!

Only d roots.

Lemma 1: $P(x)$ has root a iff $P(x)/(x-a)$ has remainder 0: $P(x) = (x-a)Q(x)$.

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

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:

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: $P(a)$

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: $P(a) = r$

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

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: $P(a) = r = 0$. $\square$

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: $P(a) = r = 0$. $\square$

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

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: $P(a) = r = 0$. $\square$

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

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No 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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

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

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

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

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

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

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1.
$Q(x)$ has smaller degree ...
so by induction hypothesis...
we are done.

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1.
$Q(x)$ has smaller degree ...
so by induction hypothesis...
we are done. $\square$

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1.
$Q(x)$ has smaller degree ...
so by induction hypothesis...
we are done. $\square$

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

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1.
$Q(x)$ has smaller degree ...
so by induction hypothesis...
we are done. $\square$

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

The contrapositive...

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: $P(a) = r = 0$. $\square$

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

Proof Sketch: By induction.

Base Case: degree 0. No roots.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1.
$Q(x)$ has smaller degree ...
so by induction hypothesis...
we are done. $\square$

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

The contrapositive...

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

Summary.

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

Summary.

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

Existence:

Summary.

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

Existence:

Lagrange Interpolation.

Summary.

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

Existence:

Lagrange Interpolation.

Uniqueness:

Summary.

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

Existence:

Lagrange Interpolation.

Uniqueness:

At most d roots for degree d polynomial.

Finite Fields

Proof works for reals, rationals, and complex numbers.

Finite Fields

Proof works for reals, rationals, and complex numbers.

..but not for integers, since no 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..

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.

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.

Finite Fields

Proof works for reals, rationals, and complex numbers.

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

Arithmetic modulo a prime p has multiplicative inverses..

..and has only a finite number of elements.

Good for computer science.

Arithmetic modulo a prime p is a **finite field** denoted by F_p or $GF(p)$.

Finite Fields

Proof works for reals, rationals, and complex numbers.

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

Arithmetic modulo a prime p has multiplicative inverses..

..and has only a finite number of elements.

Good for computer science.

Arithmetic modulo a prime p is a **finite field** denoted by F_p or $GF(p)$.

Intuitively, a field is a set with operations corresponding to addition, multiplication, and division.

Secret Sharing

Modular Arithmetic Fact: Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d+1$ points.

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 random $a_1, \ldots, a_{k-1}$.

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 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 $a_0 = s$.

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 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 $(i, P(i) \mod p)$.

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 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 $(i, P(i) \mod p)$.

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 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 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 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 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 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 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 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 knows secret.
Knowing k pts, only one $P(x)$, evaluate $P(0)$.
Secrecy: Any $k-1$ knows nothing.
Knowing $\leq k-1$ pts, any $P(0)$ is possible.
Efficiency: ???

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 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 knows secret.
Knowing k pts, only one $P(x)$, evaluate $P(0)$.
Secrecy: Any $k-1$ knows nothing.
Knowing $\leq k-1$ pts, any $P(0)$ is possible.
Efficiency: ???

Efficiency.

Efficiency.

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

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.
Minimal!

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.
Minimal!

With k shares, reconstruct polynomial, $P(x)$.

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.
Minimal!

With k shares, reconstruct polynomial, $P(x)$.

With $k-1$ shares, any of p values possible for $P(0)$!

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.
Minimal!

With k shares, reconstruct polynomial, $P(x)$.

With $k-1$ shares, any of p values possible for $P(0)$!

(Within 1 bit of) any b-bit string possible!

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.
Minimal!

With k shares, reconstruct polynomial, $P(x)$.

With $k-1$ shares, any of p values possible for $P(0)$!

(Within 1 bit of) any b-bit string possible!

(Within 1 bit of) b-bits are missing: one $P(i)$.

Efficiency.

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

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.

Working over numbers within 1 bit of secret size.
Minimal!

With k shares, reconstruct polynomial, $P(x)$.

With $k-1$ shares, any of p values possible for $P(0)$!

(Within 1 bit of) any b-bit string possible!

(Within 1 bit of) b-bits are missing: one $P(i)$.

Within 1 of optimal number of bits.

Runtime.

Runtime.

Runtime: polynomial in k, n, and $\log p$.

1. Evaluate degree $n-1$ polynomial $n+k$ times using $\log p$-bit numbers. $O(kn\log^2 p)$.

Runtime.

Runtime: polynomial in k, n, and $\log p$.

1. Evaluate degree $n-1$ polynomial $n+k$ times using $\log p$-bit numbers. $O(kn\log^2 p)$.
2. Reconstruct secret by solving system of n equations using $\log p$-bit arithmetic. $O(n^3\log^2 p)$.

Runtime.

Runtime: polynomial in k, n, and $\log p$.

1. Evaluate degree $n-1$ polynomial $n+k$ times using $\log p$-bit numbers. $O(kn\log^2 p)$.
2. Reconstruct secret by solving system of n equations using $\log p$-bit arithmetic. $O(n^3\log^2 p)$.
3. Matrix has special form so $O(n\log n\log^2 p)$ reconstruction.

Runtime.

Runtime: polynomial in k, n, and $\log p$.

1. Evaluate degree $n-1$ polynomial $n+k$ times using $\log p$-bit numbers. $O(kn\log^2 p)$.
2. Reconstruct secret by solving system of n equations using $\log p$-bit arithmetic. $O(n^3\log^2 p)$.
3. Matrix has special form so $O(n\log n\log^2 p)$ reconstruction.

Faster versions in practice are almost as efficient.

A bit of counting.

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

A bit of counting.

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

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

A bit of counting.

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

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

A bit of counting.

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

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

Infinite number for reals, rationals, complex numbers!

Erasure Codes.

Satellite

GPS device

Erasure Codes.

Satellite

3 packet message.

GPS device

Erasure Codes.

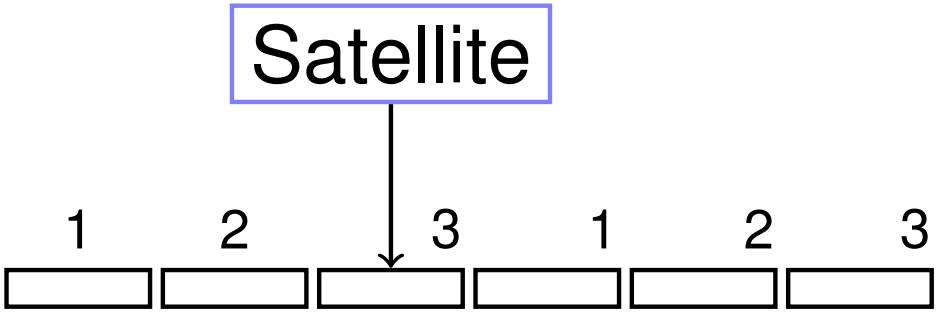
Satellite

3 packet message.

Lose 3 out 6 packets.

GPS device

Erasure Codes.

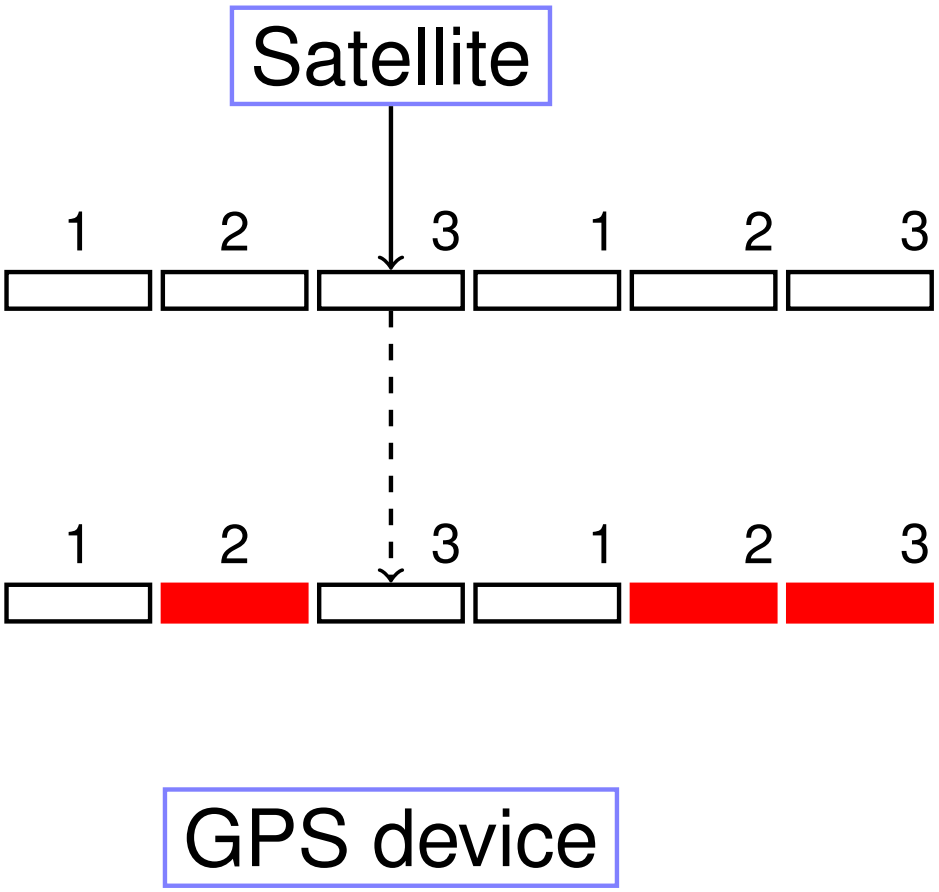


3 packet message. So send 6!

Lose 3 out 6 packets.

GPS device

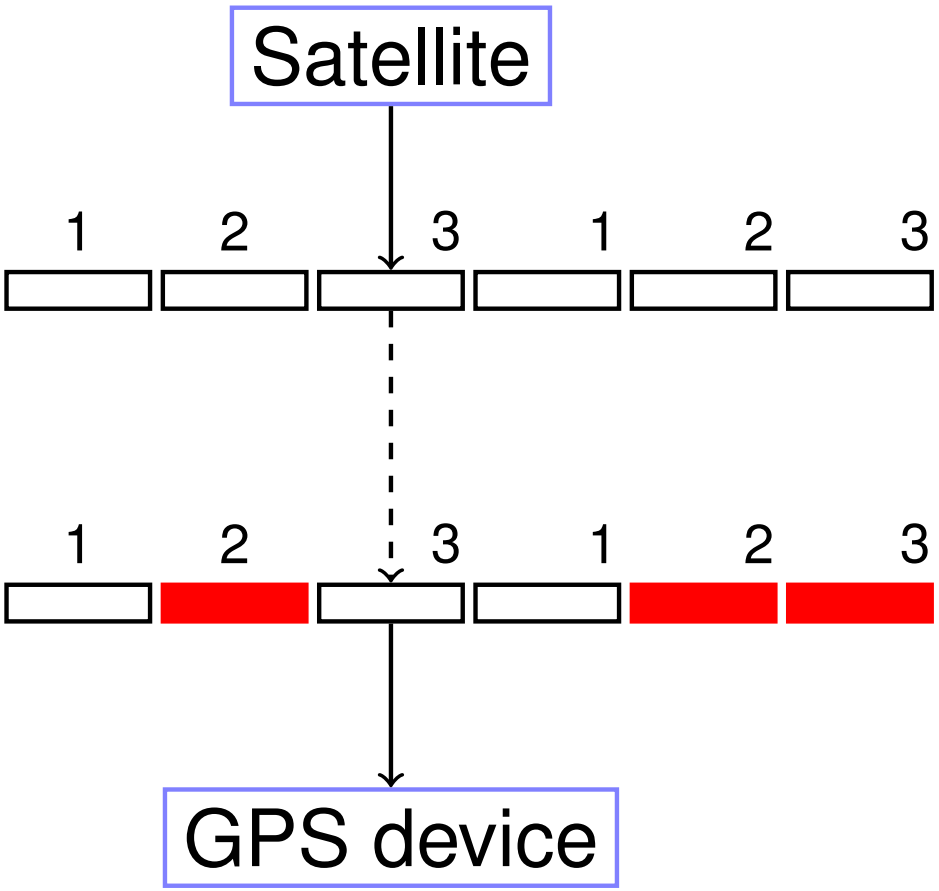
Erasure Codes.



3 packet message. So send 6!

Lose 3 out 6 packets.

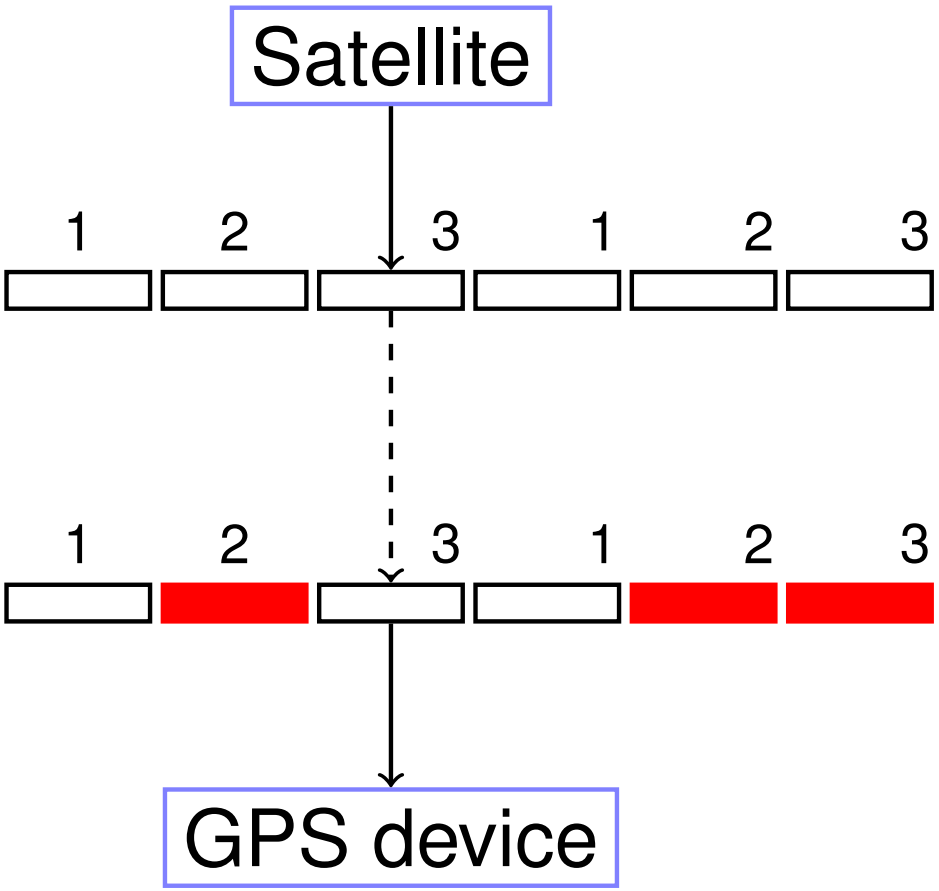
Erasure Codes.



3 packet message. So send 6!

Lose 3 out 6 packets.

Erasure Codes.



3 packet message. So send 6!

Lose 3 out 6 packets.

Gets packets 1,1,and 3.

Problem: Want to send a message with n packets.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

Question: Can you send $n+k$ packets and recover message?

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

Question: Can you send $n+k$ packets and recover message?

On Friday!