Today.

Polynomials.

Today.

Polynomials.

Secret Sharing.

Today.

Polynomials.

Secret Sharing.

Erasure Coding.

Secret Sharing.

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.
Robustness: 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.

Secret Sharing.

Share secret among n people.

Secrecy: Any $k-1$ knows nothing.
Robustness: Any k knows secret.
Efficient: Minimize storage.

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

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

TYPE OF CODE	REED-SOLOMON	LOW-DENSITY PARITY-CHECK (LDPC)	TURBO
APPLICA-TIONS	 DATA STORAGE (CD/DVD)	 WIFI, BROADCASTING	 CELLULAR (3G, 4G), SATELLITE COMMUNICATIONS

Back to secret sharing: idea of the day

Back to secret sharing: idea of the day

Two points make a line.

Back to secret sharing: idea of the day

Two points make a line.

Lots of lines go through one point.

Back to secret sharing: idea of the day

Two points make a line.

Lots of lines go through one point.

Secret message is represented as the y-intercept.

Back to secret sharing: idea of the day

Two points make a line.

Lots of lines go through one point.

Secret message is represented as the y-intercept.

Let's recall how polynomials work.

Back to secret sharing: idea of the day

Two points make a line.

Lots of lines go through one point.

Secret message is represented as the y-intercept.

Let's recall how polynomials work.

Polynomials

A **polynomial**

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

is specified by **coefficients** $a_d, \ldots a_0$.

---

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

Polynomials

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 $b = P(a)$.

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

Polynomials

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: $a_1, \ldots, a_d \in \Re$, use $x \in \Re$.

---

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

Polynomials

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: $a_1, \ldots, a_d \in \Re$, use $x \in \Re$.

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

---

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

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

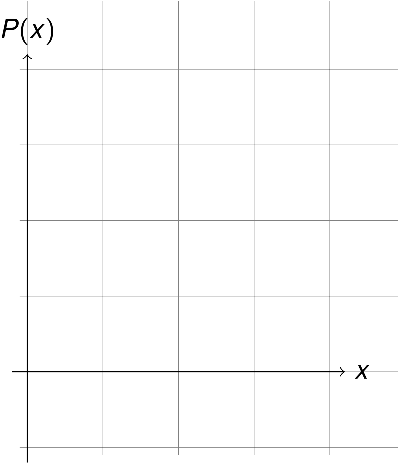
Line: $P(x) = a_1 x + a_0$

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

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

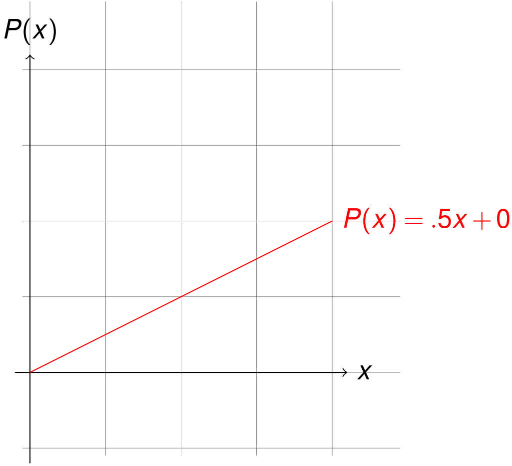
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



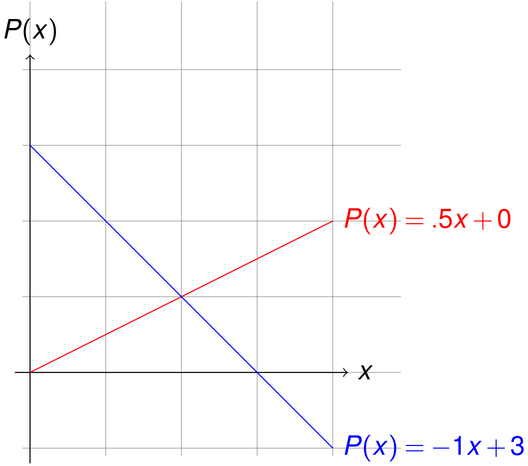
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



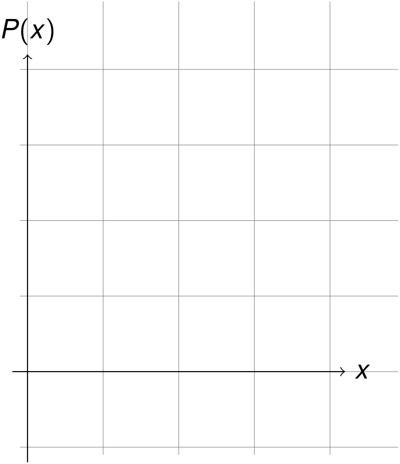
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



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

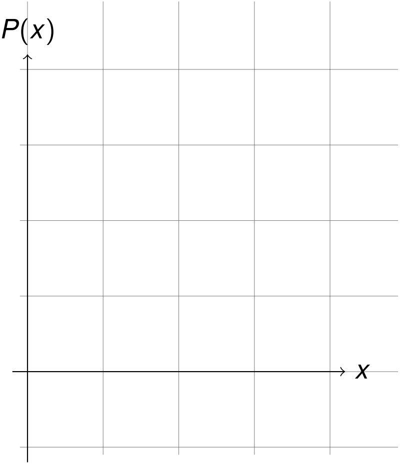
Line: $P(x) = a_1 x + a_0 = mx + b$



Parabola: $P(x) = a_2 x^2 + a_1 x + a_0$

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

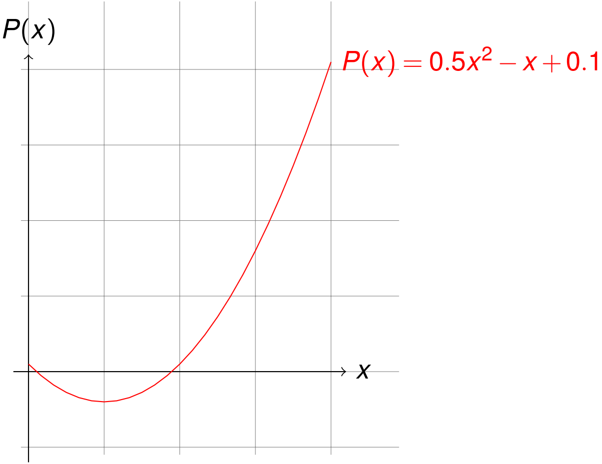
Line: $P(x) = a_1 x + a_0 = mx + b$



Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

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

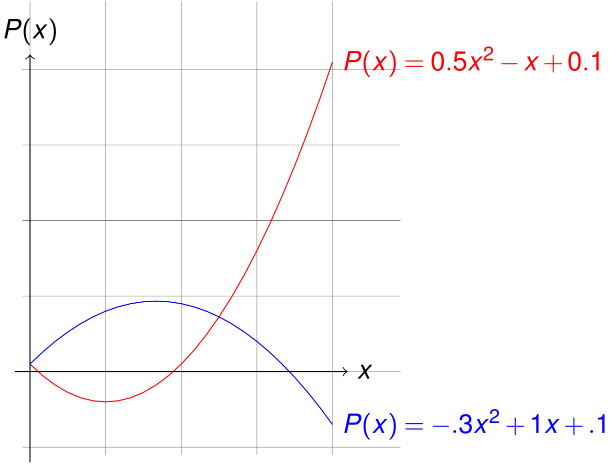
Line: $P(x) = a_1 x + a_0 = mx + b$



Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

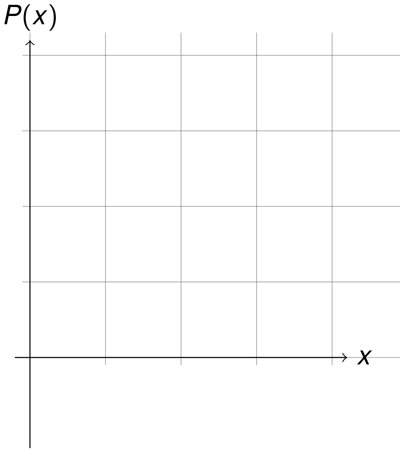
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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

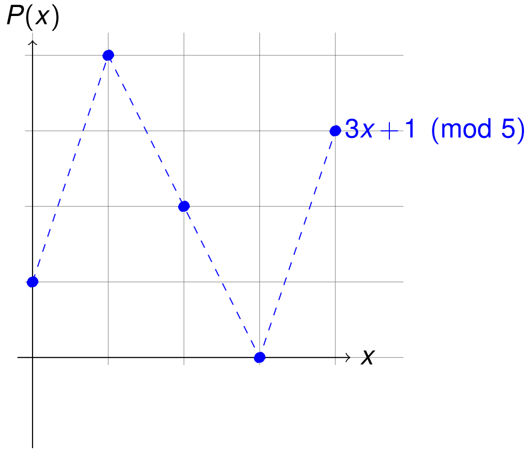


Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

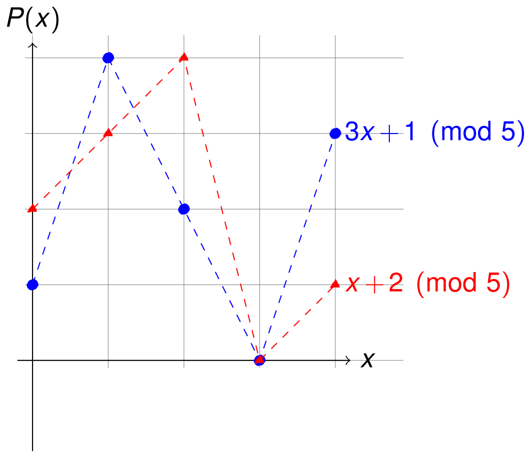
Polynomial: $P(x) = a_d x^4 + \cdots + a_0 \pmod{p}$



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



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

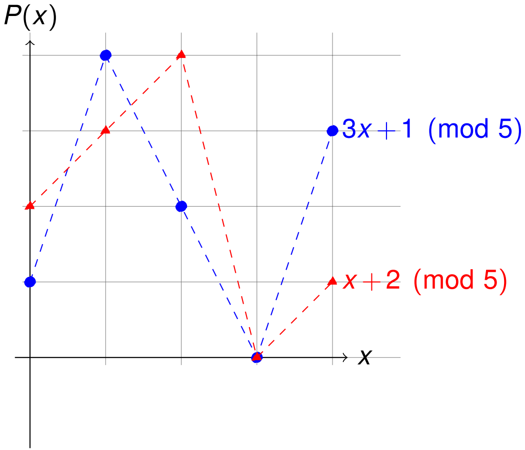


Finding an intersection.

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

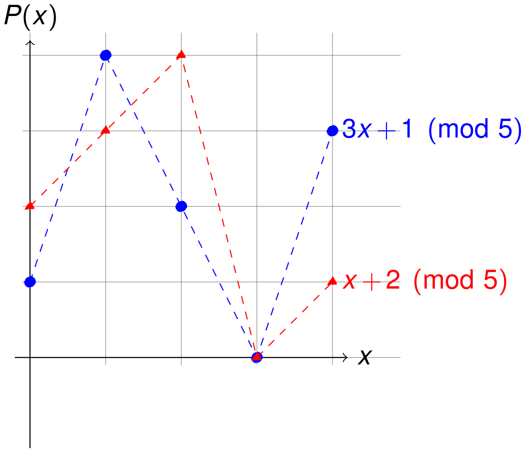
$\implies 2x \equiv 1 \pmod{5}$

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



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.

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: There is exactly 1 polynomial having degree $\leq d$ containing $d+1$ points. [2]

[2] Points with different x values.

Two points make a line.

Fact: There is exactly 1 polynomial having degree $\leq d$ containing $d+1$ points. [2]

Two points specify a line.

[2] Points with different x values.

Two points make a line.

Fact: There is exactly 1 polynomial having degree $\leq d$ containing $d+1$ points. [2]

Two points specify a line. Three points specify a parabola.

[2] Points with different x values.

Two points make a line.

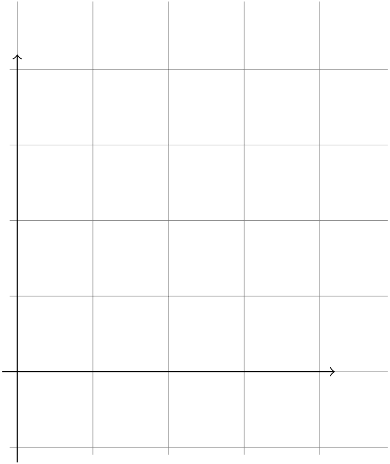
Fact: There is exactly 1 polynomial having degree $\leq d$ containing $d+1$ points. [2]

Two points specify a line. Three points specify a parabola.

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

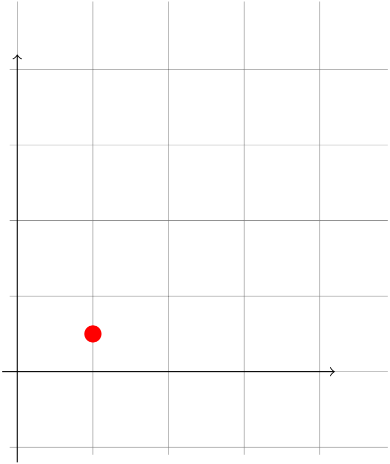
[2] Points with different x values.

3 points determine a parabola.



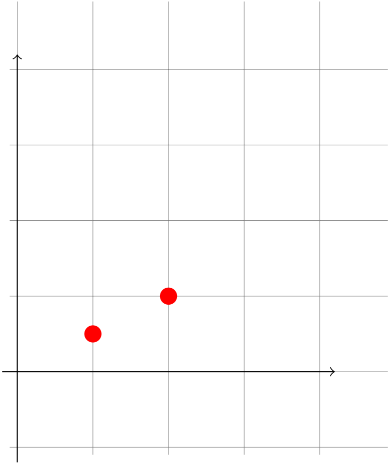
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



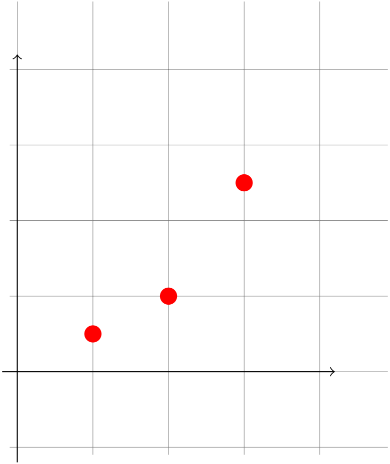
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



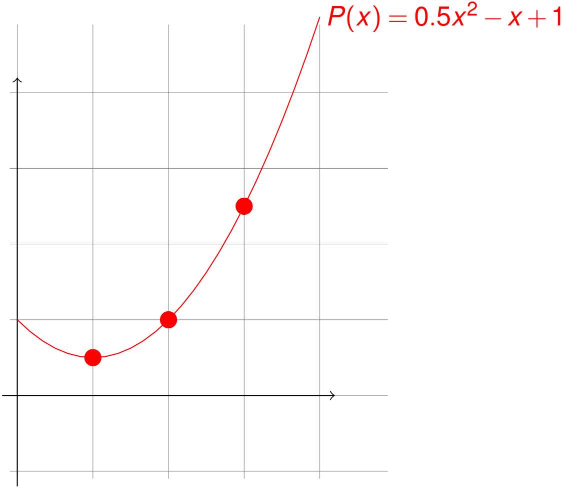
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



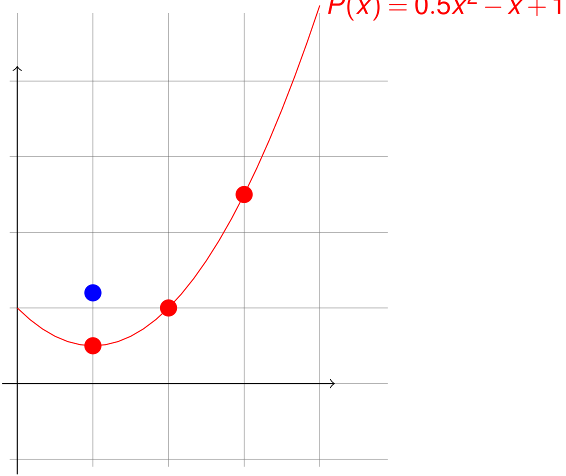
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



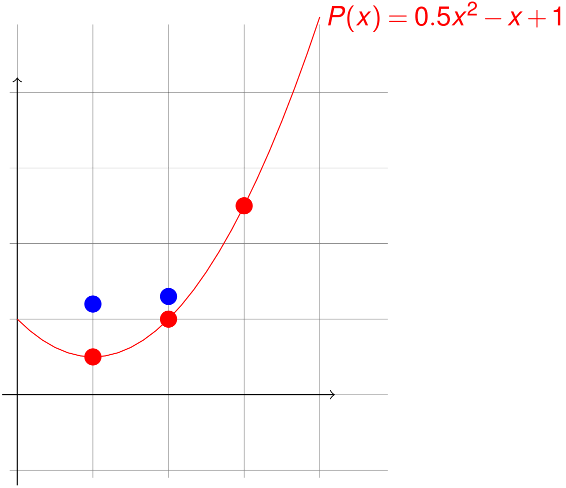
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



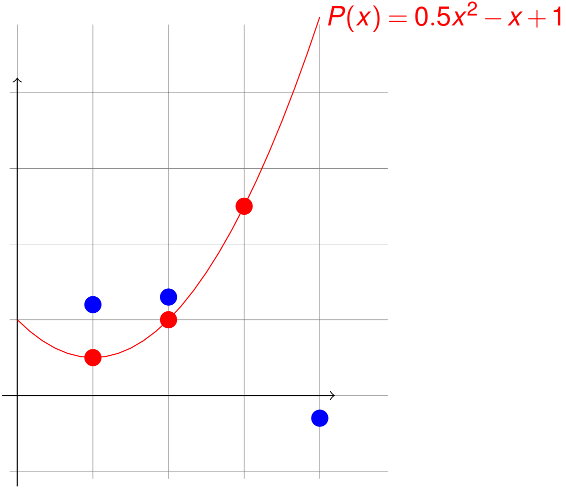
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



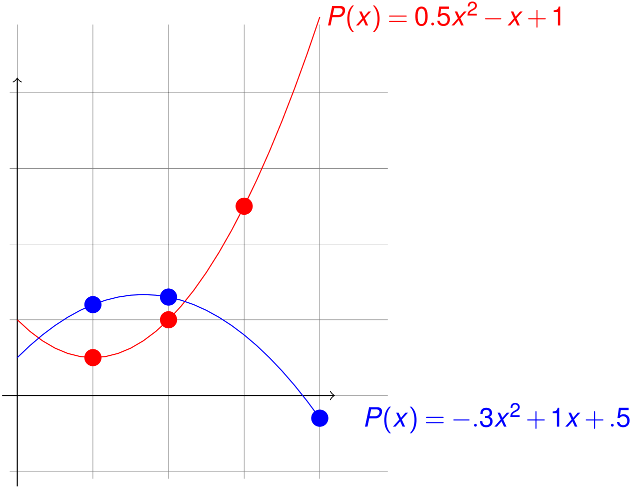
Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



Fact: Exactly 1 polynomial having degree$\leq d$ polynomial contains $d+1$ points. [3]

[3] Points with different x values.

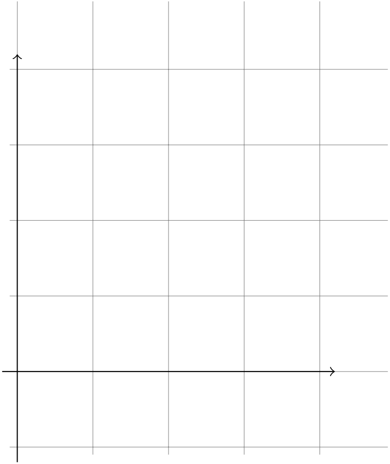
2 points not enough.

2 points not enough.

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

2 points not enough.

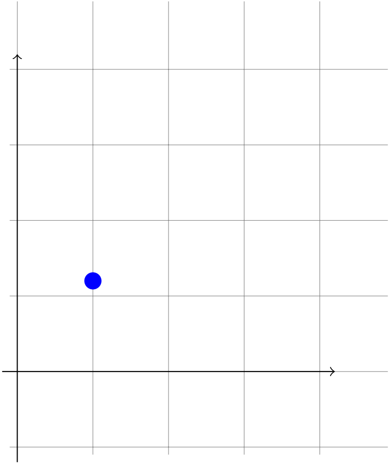
Question: How many parabolas exist that contain exactly 2 distinct points?



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

2 points not enough.

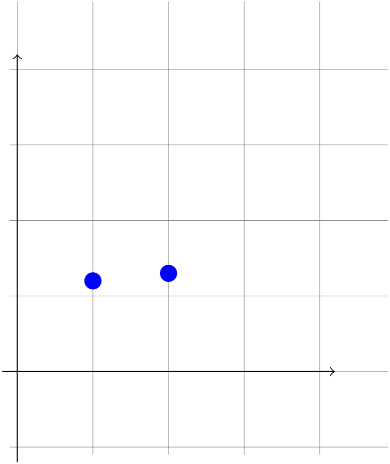
Question: How many parabolas exist that contain exactly 2 distinct points?



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

2 points not enough.

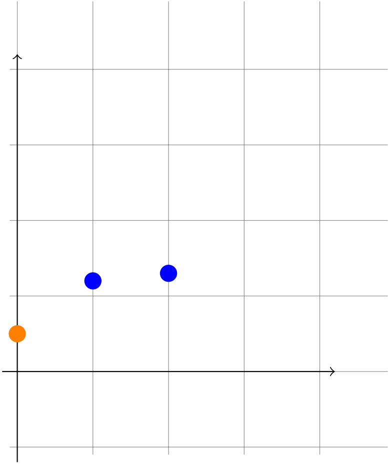
Question: How many parabolas exist that contain exactly 2 distinct points?



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

2 points not enough.

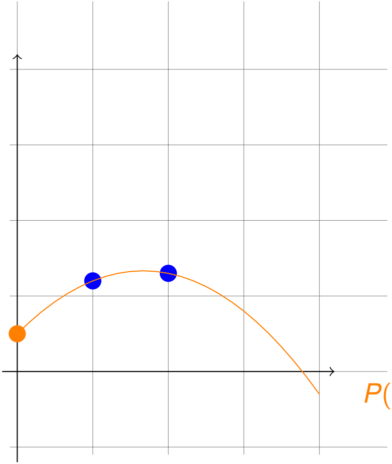
Question: How many parabolas exist that contain exactly 2 distinct points?



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

2 points not enough.

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

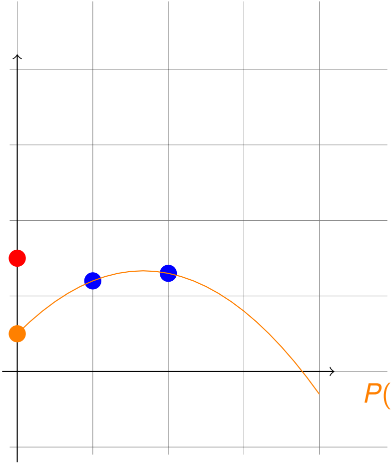


$P(x) = -.3x^2 + 1x + .5$

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

2 points not enough.

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

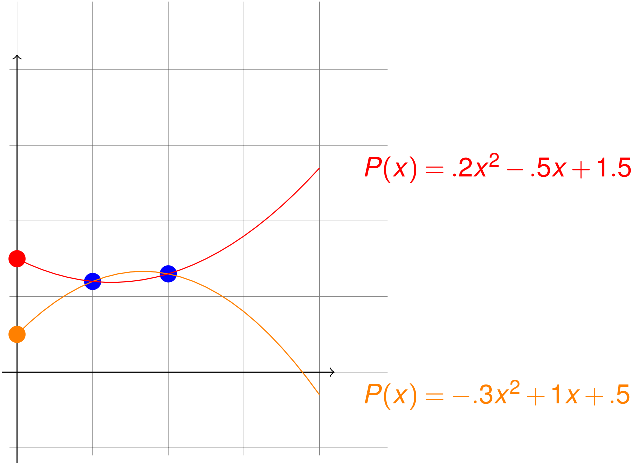


$P(x) = -.3x^2 + 1x + .5$

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

2 points not enough.

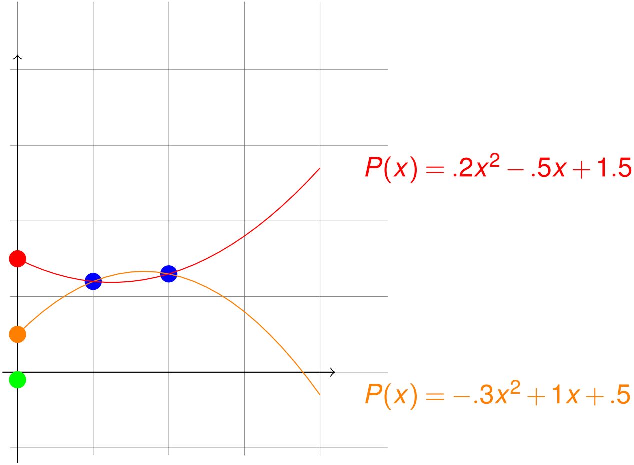
Question: How many parabolas exist that contain exactly 2 distinct points?



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

2 points not enough.

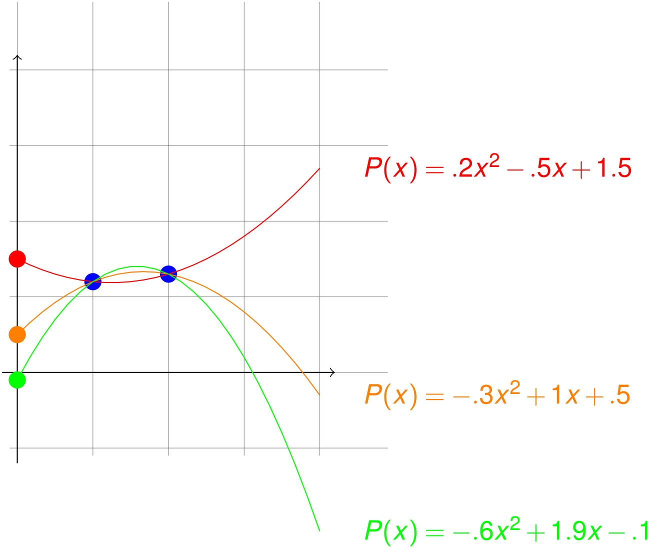
Question: How many parabolas exist that contain exactly 2 distinct points?



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

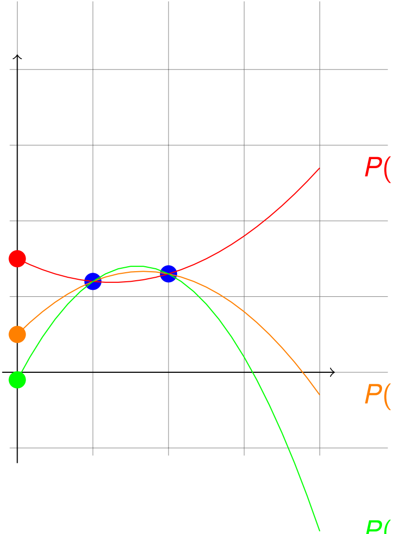
2 points not enough.

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



2 points not enough.

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



$P(x) = .2x^2 - .5x + 1.5$

$P(x) = -.3x^2 + 1x + .5$

$P(x) = -.6x^2 + 1.9x - .1$

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

Modular Arithmetic Fact and Secrets

Modular Arithmetic Fact and Secrets

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

Modular Arithmetic Fact and Secrets

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

Shamir's k out of n Scheme:

Modular Arithmetic Fact and Secrets

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

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

Modular Arithmetic Fact and Secrets

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

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

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

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and random $a_1,\ldots,a_{k-1}$.
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 polynomial having degree $\leq d$ with arithmetic modulo prime p contains $d+1$ pts.

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

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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: Exactly 1 polynomial having degree $\leq d$ with arithmetic modulo prime p contains $d+1$ pts.

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

1. Choose $a_0 = s$, and random $a_1,\ldots,a_{k-1}$.
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: Exactly 1 polynomial having degree $\leq d$ with arithmetic modulo prime p contains $d+1$ pts.

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

1. Choose $a_0 = s$, and random $a_1, \dots, a_{k-1}$.
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.

Modular Arithmetic Fact and Secrets

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

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

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

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and random $a_1,\ldots,a_{k-1}$.
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 polynomial having degree $\leq d$ with arithmetic modulo prime p contains $d+1$ pts.

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

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
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 polynomial having degree $\leq d$ with arithmetic modulo prime p contains $d+1$ pts.

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

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

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and random $a_1, \dots, a_{k-1}$.
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

Modular Arithmetic Fact and Secrets

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

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

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

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

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

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

From $d+1$ points to degree d polynomial?

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

From $d+1$ points to degree d polynomial?

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

$$P(1) =$$

From $d+1$ points to degree d polynomial?

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

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

From $d+1$ points to degree d polynomial?

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

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

From $d+1$ points to degree d polynomial?

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

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

From $d+1$ points to degree d polynomial?

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

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

From $d+1$ points to degree d polynomial?

For a line, $a_1x+a_0 = mx+b$ 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..

From $d+1$ points to degree d polynomial?

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

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

Subtract first from second..

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

From $d+1$ points to degree d polynomial?

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

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

Subtract first from second..

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

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

From $d+1$ points to degree d polynomial?

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

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

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.

From $d+1$ points to degree d polynomial?

For a line, $a_1x+a_0 = mx+b$ 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, $a_2 x^2 + a_1 x + a_0$ 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.

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

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.

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

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ 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...

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

In general..

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

Solve...

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

Will this always work?

In general..

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

Solve...

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

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...

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

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...

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

Will this always work?

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

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

Another Construction: Lagrange Interpolation!

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

Another Construction: Lagrange Interpolation!

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

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

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

Value is 0 at 2 and 3.

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

Value is 0 at 2 and 3. Value is 2 at 1.

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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).

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

$P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

$P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

$P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?

...after a lot of calculations...

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

$P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?

...after a lot of calculations... $P(x) = 2x^2 + 1x + 4 \mod 5$.

Another Construction: Lagrange Interpolation!

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

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

Try $(x-2)(x-3) \pmod 5$.

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

$P(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$ works.

Same as before?

...after a lot of calculations... $P(x) = 2x^2 + 1x + 4 \mod 5$.

The same as before!

Polynomials.

We will work with polynomials with arithmetic modulo p.

Polynomials.

We will work with polynomials with arithmetic modulo *p*.

Everything has a multiplicative inverse.

Polynomials.

We will work with polynomials with arithmetic modulo p.

Everything has a multiplicative inverse.

Like rationals, reals.

Polynomials.

We will work with polynomials with arithmetic modulo p.

Everything has a multiplicative inverse.

Like rationals, reals.

Warning: no calculus,

Polynomials.

We will work with polynomials with arithmetic modulo *p*.

Everything has a multiplicative inverse.

Like rationals, reals.

Warning: no calculus, and no order even.

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, $x_1, \ldots, x_{d+1}$.

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

Delta Polynomials: Concept.

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

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

Given $d+1$ points, use Δ_i functions to go through points?

Delta Polynomials: Concept.

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

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

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

Delta Polynomials: Concept.

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

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

Given $d+1$ points, use Δ_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, $x_1, \ldots, x_{d+1}$.

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

Given $d+1$ points, use Δ_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, $x_1, \ldots, x_{d+1}$.

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

Given $d+1$ points, use Δ_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, $x_1, \ldots, x_{d+1}$.

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

Given $d+1$ points, use Δ_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, $x_1, \dots, x_{d+1}$.

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

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

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, $x_1, \ldots, x_{d+1}$.

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

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

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

Given $d+1$ points, use Δ_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, $x_1,\ldots,x_{d+1}$.

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

Given $d+1$ points, use Δ_i functions to go through points?
(x_1,y_1), ..., (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 Δ_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 polynomial having degree $\leq d$ with arithmetic modulo prime p contains $d + 1$ pts.

There exists a polynomial...

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

There exists a polynomial...

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

There exists a polynomial...

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

Numerator is 0 at $x_j \neq x_i$.

There exists a polynomial...

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

Numerator is 0 at $x_j \neq x_i$.

Denominator makes it 1 at x_i.

There exists a polynomial...

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

Numerator is 0 at $x_j \neq x_i$.

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

Numerator is 0 at $x_j \neq x_i$.

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

Numerator is 0 at $x_j \neq x_i$.

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

Proof of at least one polynomial:
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

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

Numerator is 0 at $x_j \neq x_i$.

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!

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.

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

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

Work modulo 5.

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

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 $(3,0)$.

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

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 $(3,0)$.

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

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 $(3,0)$.

$$\Delta_1(x) = \frac{(x-3)}{1-3} = \frac{x-3}{-2}$$
$$= 2(x-3) = 2x - 6$$

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 $(3,0)$.

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

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 $(3,0)$.

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

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

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 $(3,0)$.

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

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

Work modulo 5.

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 $(3,0)$.

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

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

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 $(3,0)$.

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

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

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

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 $(3,0)$.

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

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 $(3,0)$.

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

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

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

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 $(3,0)$.

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

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

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

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 $(3,0)$.

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

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

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

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 $(3,0)$.

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

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

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

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

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

Numerator is 0 at $x_j \neq x_i$.

In general.

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

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

Numerator is 0 at $x_j \neq x_i$.

Denominator makes it 1 at x_i.

In general.

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

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

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

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

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!

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

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

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

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m, n)=1.

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m, n)=1.

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m,n)=1.

Solution: $x = au + bv$, where

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m, n)=1.

Solution: $x = au + bv$, where

$u = 0 \pmod{n}$ and $u = 1 \pmod{m}$

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m, n)=1.

Solution: $x = au + bv$, where

$u = 0 \pmod{n}$ and $u = 1 \pmod{m}$
$v = 1 \pmod{n}$ and $v = 0 \pmod{m}$

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m, n)=1.

Solution: $x = au + bv$, where

$u = 0 \pmod{n}$ and $u = 1 \pmod{m}$
$v = 1 \pmod{n}$ and $v = 0 \pmod{m}$

Similar deal here with the Delta polynomials in Lagrange interpolation.

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

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

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m, n)=1.

Solution: $x = au + bv$, where

$u = 0 \pmod{n}$ and $u = 1 \pmod{m}$
$v = 1 \pmod{n}$ and $v = 0 \pmod{m}$

Similar deal here with the Delta polynomials in Lagrange interpolation.

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.

Proof:

Uniqueness.

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

Proof:

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

Uniqueness.

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

Proof:

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

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

Uniqueness.

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

Proof:

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

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

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

Uniqueness.

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

Proof:

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

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

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

Uniqueness.

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

Proof:

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

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

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

$\square$

Uniqueness.

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

Proof:

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

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

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

□

Must prove **Roots fact.**

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

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: $P(x) = (x-a)Q(x) + r$.
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: $P(a) = r$.
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 $r = 0$.

$\square$

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: $P(a) = r$.
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.

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.

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.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1. $Q(x)$ has smaller degree so use the 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: $P(a) = r$.
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. □

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.

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 $d+1$.

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.

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.

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 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..

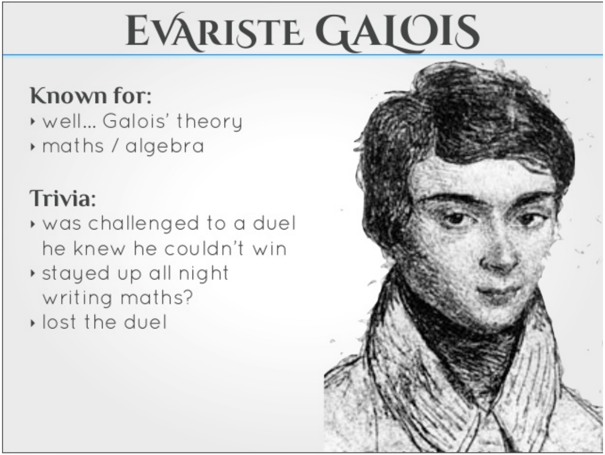
..and has only a finite number of elements.

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.

History lesson: Evariste Galois (1811-1832)



lundi 11 février 2013

History lesson: Evariste Galois (1811-1832)

Évariste Galois

From Wikipedia, the free encyclopedia

"Galois" redirects here. For other uses, see Gallois (disambiguation).

Évariste Galois (French: [evaʁist ɡalwa]; 25 October 1811 – 31 May 1832) was a French mathematician born in Bourg-la-Reine. While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a problem standing for 350 years. His work laid the foundations for Galois theory and group theory, two major branches of abstract algebra, and the subfield of Galois connections. He died at age 20 from wounds suffered in a duel.

Évariste Galois

A portrait of Évariste Galois aged about 15

Born	25 October 1811 Bourg-la-Reine, French Empire
Died	31 May 1832 (aged 20) Paris, Kingdom of France
Nationality	French
Alma mater	École préparatoire (no degree)
Known for	Work on the theory of equations and Abelian integrals
Scientific career	
Fields	Mathematics
Signature	

Contents [hide]

Life [edit]

Early life [edit]

Galois was born on 25 October 1811 to Nicolas-Gabriel Galois and Adélaïde-Marie (born Demante).[1] His father was a Republican and was head of Bourg-la-Reine's liberal party. His father became mayor of the village after Louis XVIII returned to the throne in 1814. His mother, the daughter of a jurist, was a fluent reader of Latin and classical literature and was responsible for her son's education for his first twelve years. At the age of 10, Galois was offered a place at the college of Reims, but his mother preferred to keep him at home.

In October 1823, he entered the Lycée Louis-le-Grand, and despite some turmoil in the school at the beginning of the term (when about a hundred students were

Secret Sharing

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

Secret Sharing

Modular Arithmetic Fact: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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 $a_0 = s$.

Secret Sharing

Modular Arithmetic Fact: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: There exists exactly one polynomial having 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: $P(1) \dots P(n)$.

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: $P(1) \dots P(n)$.

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.

Runtime.

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

1. Evaluate degree $k-1$ polynomial n times using $\log p$-bit numbers.
2. Reconstruct secret by solving system of k equations using $\log p$-bit arithmetic.

Erasure Codes.

Satellite

GPS device

Erasure Codes.

Satellite

3 packet message.

GPS device

Erasure Codes.

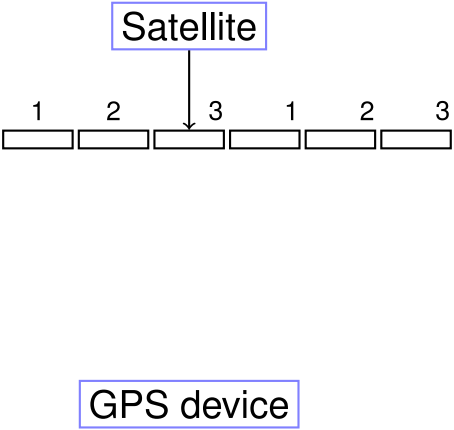
Satellite

3 packet message.

Lose 3 out 6 packets.

GPS device

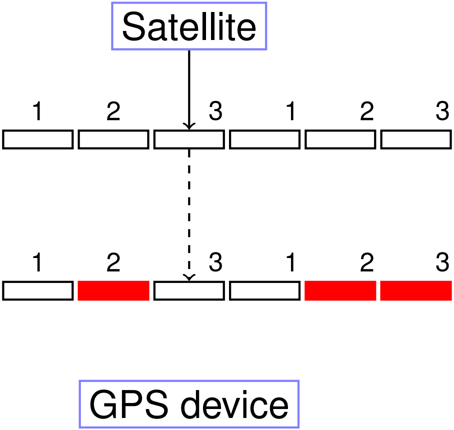
Erasure Codes.



3 packet message. So send 6!

Lose 3 out 6 packets.

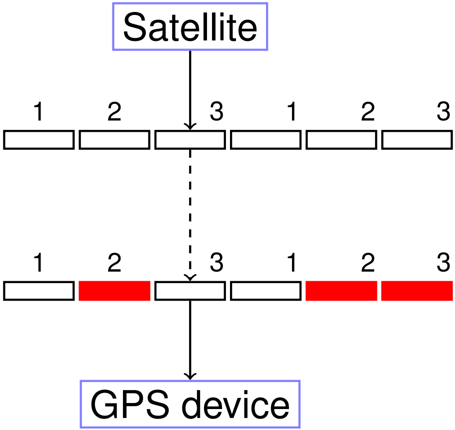
Erasure Codes.



3 packet message. So send 6!

Lose 3 out 6 packets.

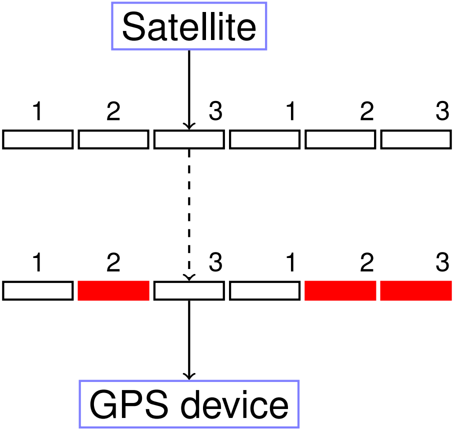
Erasure Codes.



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.

Solution Idea.

n packet message, channel that loses k packets.

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!!!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!!!!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!!!!!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!!!!!

Solution Idea.

n packet message, channel that loses k packets.

Must send $n+k$ packets!

Any n packets should allow reconstruction of n packet message.

Any n point values allow reconstruction of degree $n-1$ polynomial.

Alright!!!!!!

Use polynomials.

Erasure Codes.

Problem: Want to send a message with n packets.

Erasure Codes.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

Erasure Codes.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

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

Erasure Codes.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

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

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

Erasure Codes.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

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

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

Erasure Coding Scheme: message = $m_0, m_2, \ldots, m_{n-1}$.

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

Erasure Codes.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

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

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

Erasure Coding Scheme: message = $m_0, m_2, \ldots, m_{n-1}$.

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

Any n of the $n+k$ packets gives polynomial ...

Erasure Codes.

Problem: Want to send a message with n packets.

Channel: Lossy channel: loses k packets.

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

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

Erasure Coding Scheme: message = $m_0, m_2, \ldots, m_{n-1}$.

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

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

Erasure Codes.

Satellite

GPS device

Erasure Codes.

Satellite

n packet message.

GPS device

Erasure Codes.

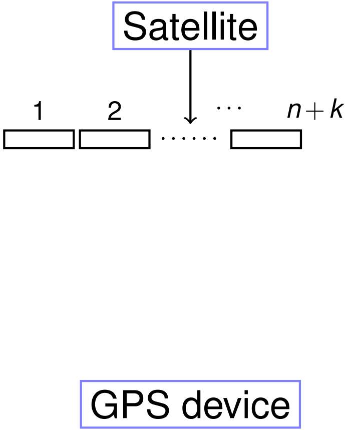
Satellite

n packet message.

Lose *k* packets.

GPS device

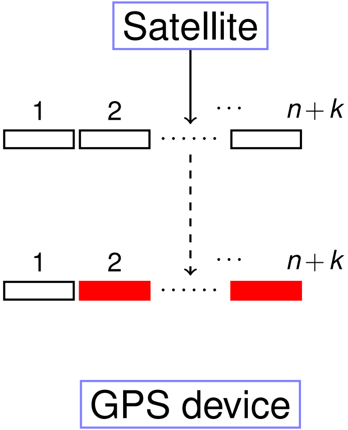
Erasure Codes.



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

Lose k packets.

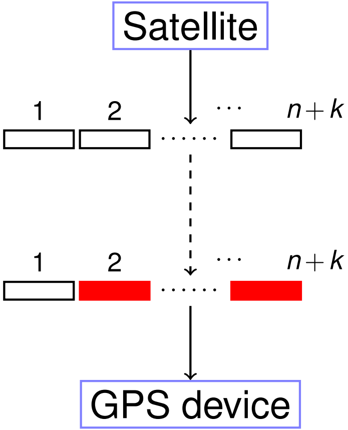
Erasure Codes.



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

Lose k packets.

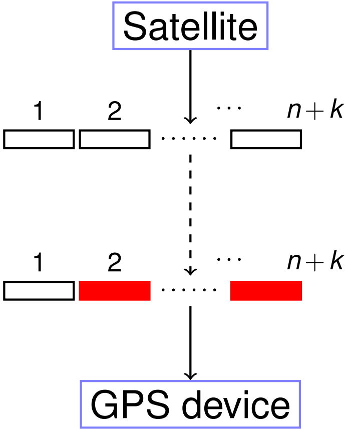
Erasure Codes.



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

Lose k packets.

Erasure Codes.

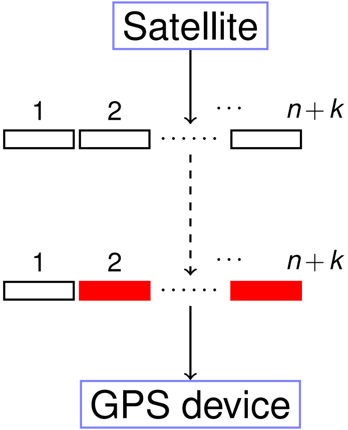


n packet message. So send $n+k$!

Lose k packets.

Any n packets is enough!

Erasure Codes.



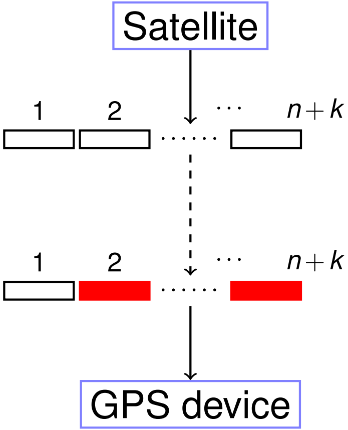
n packet message. So send $n+k$!

Lose k packets.

Any n packets is enough!

n packet message.

Erasure Codes.



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

Lose k packets.

Any n packets is enough!

n packet message.

Optimal.

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

– Can also run the Fast Fourier Transform.

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

– Can also run the Fast Fourier Transform.

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

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

– Can also run the Fast Fourier Transform.

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

Comparison with Secret Sharing: information content.

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

– Can also run the Fast Fourier Transform.

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

Comparison with Secret Sharing: information content.

Secret Sharing: each share is size of whole secret.

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

– Can also run the Fast Fourier Transform.

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

Comparison with Secret Sharing: information content.

Secret Sharing: each share is size of whole secret.
Coding: Each packet has size $1/n$ of the whole message.

Information Theory.

Size: Can choose a prime between 2^{b-1} and 2^b.
(Lose at most 1 bit per packet.)

But: packets need label for x value.

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

– Can also run the Fast Fourier Transform.

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

Comparison with Secret Sharing: information content.

Secret Sharing: each share is size of whole secret.
Coding: Each packet has size $1/n$ of the whole message.

Erasure Code: Example.

Send message of 1,4, and 4.

Erasure Code: Example.

Send message of 1,4, and 4.

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

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1$,

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4,$

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

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

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

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

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

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

6 points.

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

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

6 points. Better work modulo 7 at least!

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

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

6 points. Better work modulo 7 at least!

Why?

Erasure Code: Example.

Send message of 1,4, and 4.

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

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod 5$
$P(1) = 1, P(2) = 4, P(3) = 9 = 4 \pmod 5$

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

6 points. Better work modulo 7 at least!

Why? $(0, P(0)) = (5, P(5)) \pmod 5$

Example

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

Example

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

Modulo 7 to accommodate at least 6 packets.

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}$$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$
\begin{aligned}
P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\
P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7
\end{aligned}
$$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$
\begin{aligned}
P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod{7} \\
P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod{7} \\
P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod{7}
\end{aligned}
$$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod{7} \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod{7} \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod{7} \end{aligned}$$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod{7} \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod{7} \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod{7} \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod{7}$,

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$.

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

$P(x) = 2x^2 + 4x + 2$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

$P(x) = 2x^2 + 4x + 2$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$,

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod{7} \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod{7} \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod{7} \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod{7}$, $5a_1 + 4a_0 = 0 \pmod{7}$

$a_1 = 2a_0$. $a_0 = 2 \pmod{7}$ $a_1 = 4 \pmod{7}$ $a_2 = 2 \pmod{7}$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$, $P(2) = 4$,

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod{7} \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod{7} \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod{7} \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod{7}$, $5a_1 + 4a_0 = 0 \pmod{7}$

$a_1 = 2a_0$. $a_0 = 2 \pmod{7}$ $a_1 = 4 \pmod{7}$ $a_2 = 2 \pmod{7}$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$

Send

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod 7 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 7 \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod 7 \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod 7$, $5a_1 + 4a_0 = 0 \pmod 7$

$a_1 = 2a_0$. $a_0 = 2 \pmod 7$ $a_1 = 4 \pmod 7$ $a_2 = 2 \pmod 7$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$

Send
Packets: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Example

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

Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 1 \pmod{7} \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod{7} \\ P(3) = 2a_2 + 3a_1 + a_0 &\equiv 4 \pmod{7} \end{aligned}$$

$6a_1 + 3a_0 = 2 \pmod{7}$, $5a_1 + 4a_0 = 0 \pmod{7}$

$a_1 = 2a_0$. $a_0 = 2 \pmod{7}$ $a_1 = 4 \pmod{7}$ $a_2 = 2 \pmod{7}$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$

Send
Packets: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Notice that packets contain “x-values”.

Bad reception!

Send: $(1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)$

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)

Bad reception!

Send: $(1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

$$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod 7$$

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

$$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod 7$$
$$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod 7$$

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Channeling Sahai

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Channeling Sahai ...

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i,R(i))$.

Lagrange or linear equations.

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

Channeling Sahai ...

$P(x) = 2x^2 + 4x + 2$

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Channeling Sahai ...

$P(x) = 2x^2 + 4x + 2$

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Channeling Sahai ...

$P(x) = 2x^2 + 4x + 2$

Message?

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i)$.

Lagrange or linear equations.

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

Channeling Sahai ...

$P(x) = 2x^2 + 4x + 2$

Message? $P(1) = 1$,

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Channeling Sahai ...

$P(x) = 2x^2 + 4x + 2$

Message? $P(1) = 1, P(2) = 4,$

Bad reception!

Send: $(1,1),(2,4),(3,4),(4,7),(5,2),(6,0)$

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

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

Channeling Sahai ...

$P(x) = 2x^2 + 4x + 2$

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

Questions for Review

You want to encode a secret consisting of 1,4,4.

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

How big should modulus be?

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

How big should modulus be?

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

How big should modulus be?

Larger than 8

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

How big should modulus be?

Larger than 8 and prime!

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?

Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

How big should modulus be?

Larger than 8 and prime!

Send n packets b-bit packets, with k errors.

Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?
Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

through a noisy channel that loses 3 packets.

How big should modulus be?
Larger than 8 and prime!

Send n packets b-bit packets, with k errors.
Modulus should be larger than $n+k$ and also larger than 2^b.

Polynomials.

Polynomials.

- ..give Secret Sharing.

Polynomials.

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

Polynomials.

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

Error Correction:

Polynomials.

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

Error Correction:

Noisy Channel: corrupts k packets. (rather than loss.)

Polynomials.

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

Error Correction:

Noisy Channel: corrupts k packets. (rather than loss.)

Additional Challenge: Finding which packets are corrupt.