Today.

Polynomials.

Today.

Polynomials.

Secret Sharing.

A secret!

I have a secret!

A secret!

I have a secret!

A number from 0 to 10.

A secret!

I have a secret!

A number from 0 to 10.

What is it?

A secret!

I have a secret!

A number from 0 to 10.

What is it?

Any one of you knows nothing!

A secret!

I have a secret!

A number from 0 to 10.

What is it?

Any one of you knows nothing!
Any two of you can figure it out!

A secret!

I have a secret!

A number from 0 to 10.

What is it?

Any one of you knows nothing!
Any two of you can figure it out!

Example Applications:

A secret!

I have a secret!

A number from 0 to 10.

What is it?

Any one of you knows nothing!
Any two of you can figure it out!

Example Applications:
Nuclear launch: need at least 3 out of 5 people to launch!

A secret!

I have a secret!

A number from 0 to 10.

What is it?

Any one of you knows nothing!
Any two of you can figure it out!

Example Applications:
Nuclear launch: need at least 3 out of 5 people to launch!
Cloud service backup: several vendors, each knows nothing.

A secret!

I have a secret!

A number from 0 to 10.

What is it?

Any one of you knows nothing!
Any two of you can figure it out!

Example Applications:
Nuclear launch: need at least 3 out of 5 people to launch!
Cloud service backup: several vendors, each knows nothing.
data from any 2 to recover data.

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.
Roubustness: Any k knows secret.

Secret Sharing.

Share secret among n people.

Secrecy: Any $k-1$ knows nothing.
Roubustness: Any k knows secret.
Efficient: minimize storage.

Secret Sharing.

Share secret among n people.

Secrecy: Any $k-1$ knows nothing.
Roubustness: Any k knows secret.
Efficient: minimize storage.

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

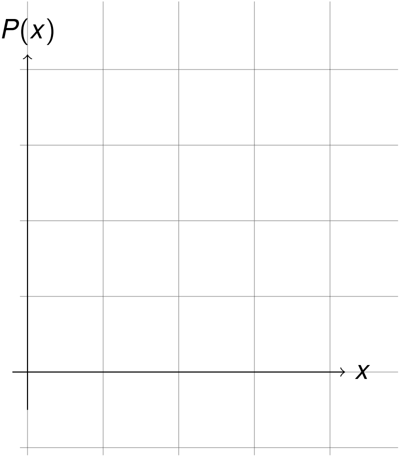
Line:$P(x) = a_1 x + a_0$

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

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

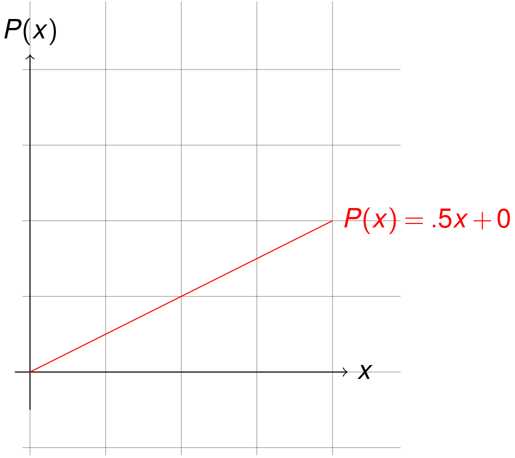
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



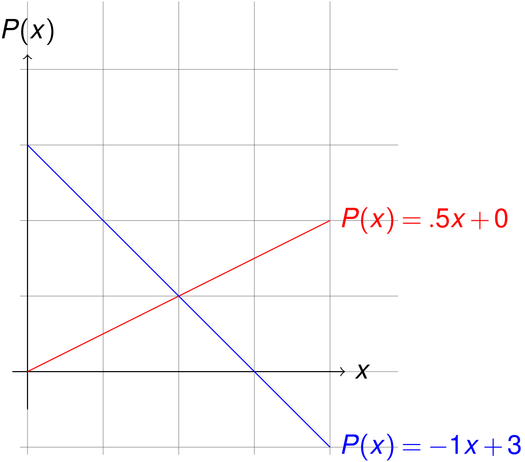
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



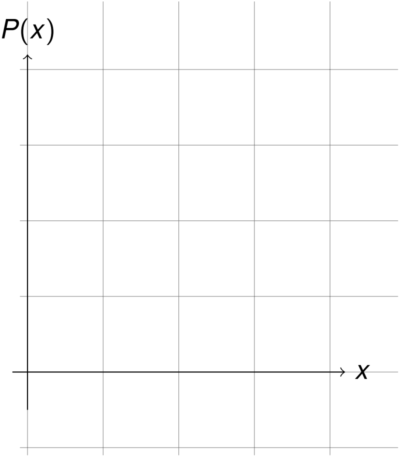
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



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

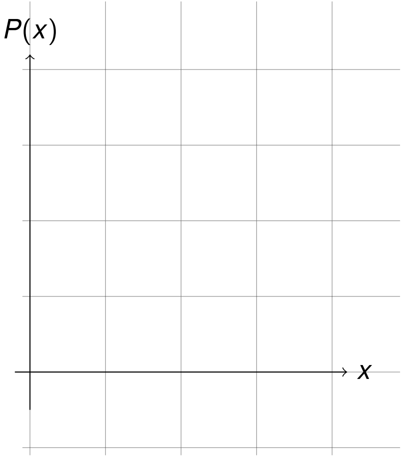
Line:$P(x) = a_1 x + a_0 = mx + b$



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

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

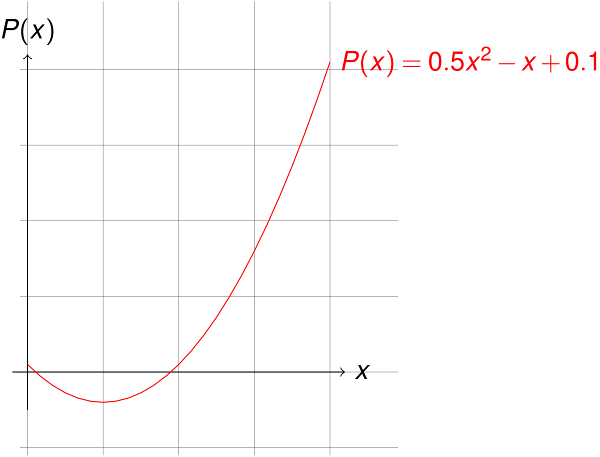
Line: $P(x) = a_1 x + a_0 = mx + b$



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

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

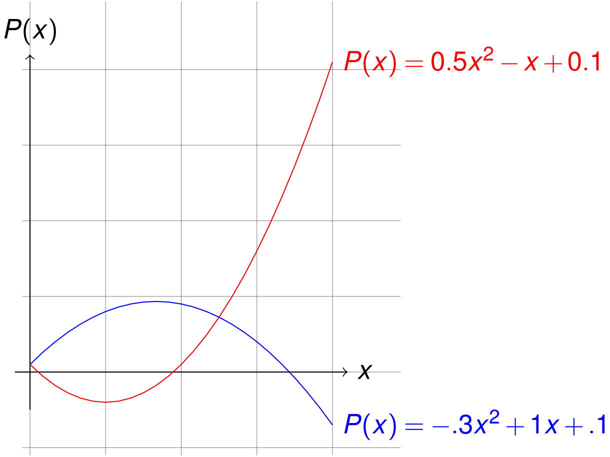
Line: $P(x) = a_1 x + a_0 = mx + b$



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

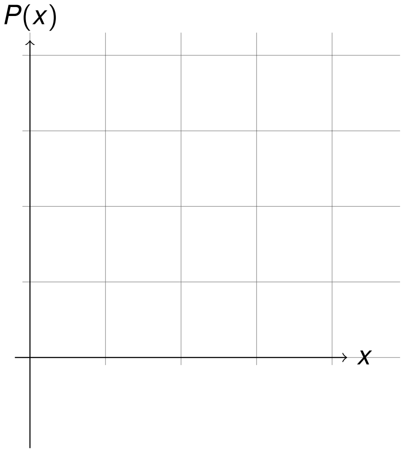
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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

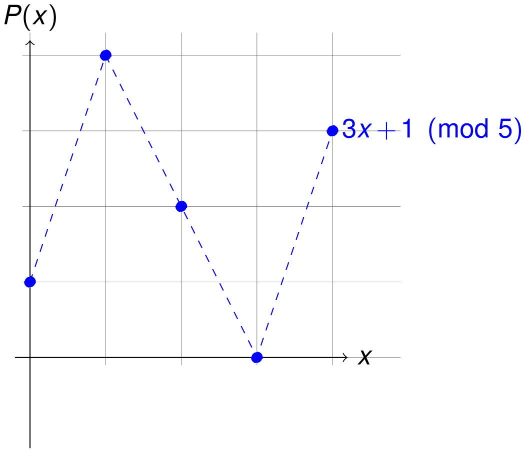


Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

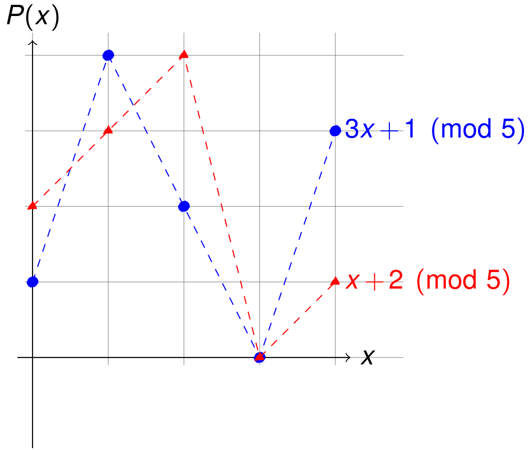
Polynomial: $P(x) = a_d x^4 + \cdots + a_0 \pmod{p}$



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



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

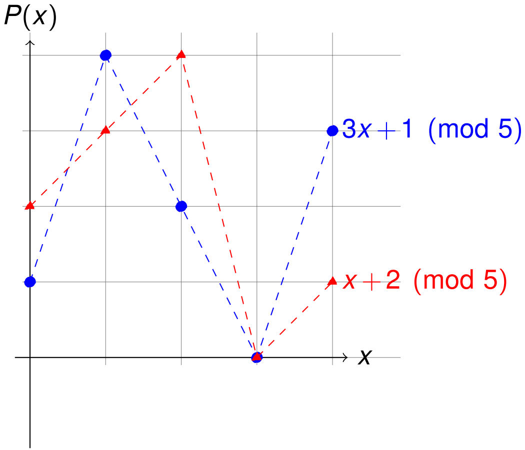


Finding an intersection.

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

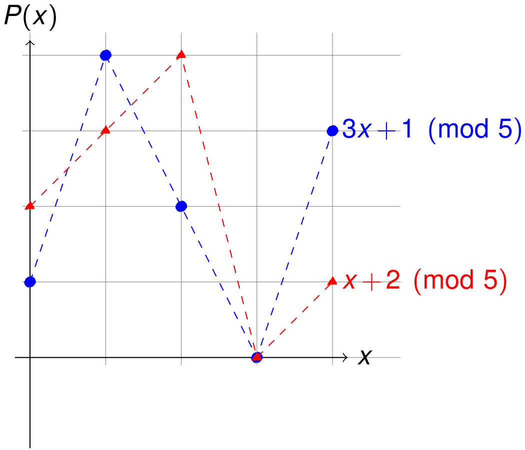
$\implies 2x \equiv 1 \pmod{5}$

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: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

[2] Points with different x values.

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line.

[2] Points with different x values.

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line. $d = 1$,

[2] Points with different x values.

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line. $d = 1$, $1 + 1$

[2] Points with different x values.

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line. $d = 1$, $1 + 1$ is 2!

[2] Points with different x values.

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line. $d = 1$, $1 + 1$ is 2!
Three points specify a parabola.

[2] Points with different x values.

Two points make a line.

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line. $d = 1$, $1 + 1$ is 2!
Three points specify a parabola. $d = 2$, $2 + 1 = 3$.

[2] Points with different x values.

Two points make a line.

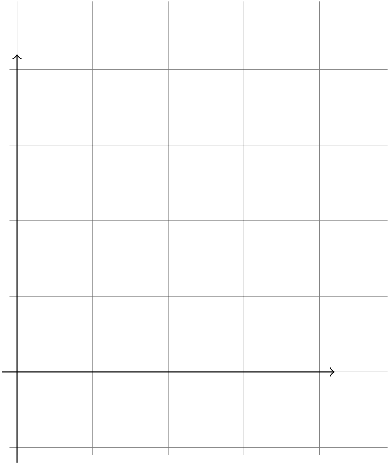
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

Two points specify a line. $d = 1$, $1 + 1$ is 2!
Three points specify a parabola. $d = 2$, $2 + 1 = 3$.

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

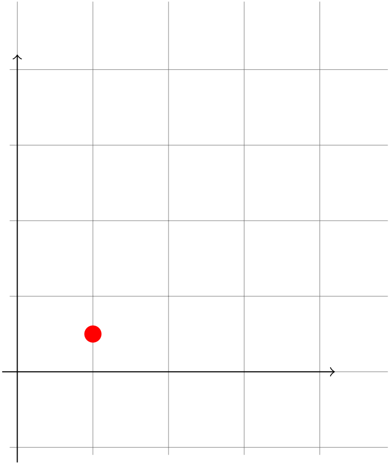
[2] Points with different x values.

3 points determine a parabola.



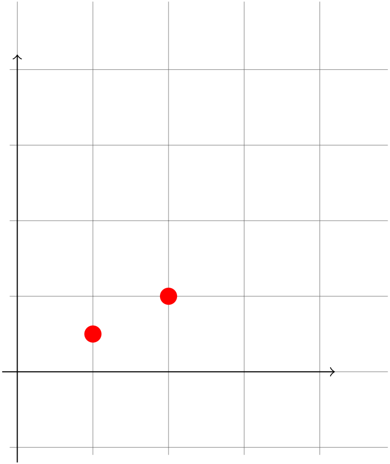
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



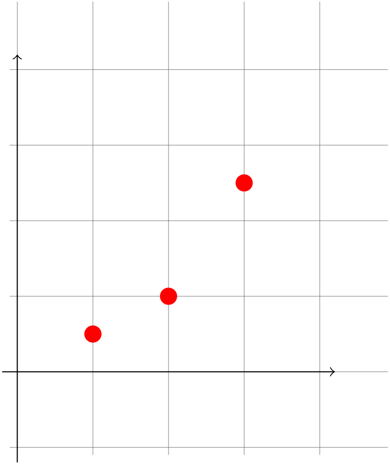
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



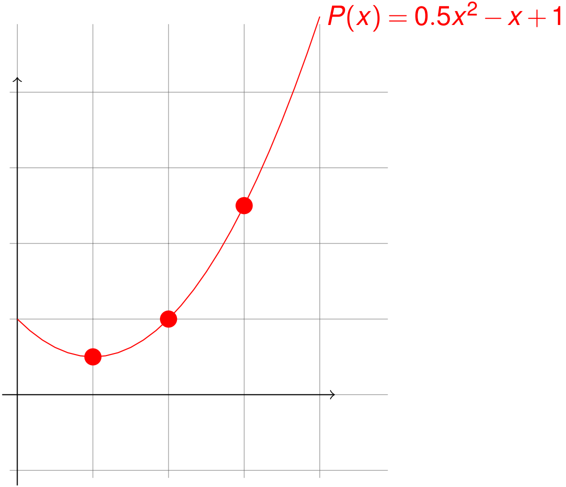
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



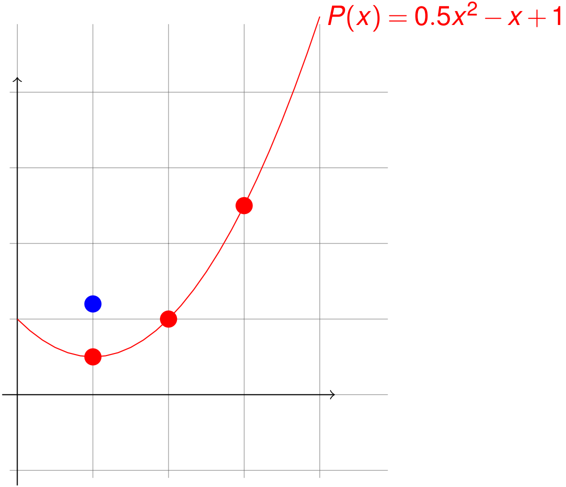
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



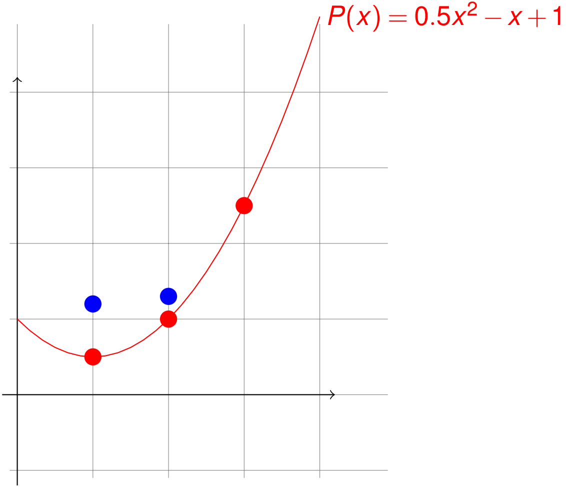
Fact: Exactly 1 degree $\leq d$ polynomial contains $d + 1$ points. [3]

3 points determine a parabola.



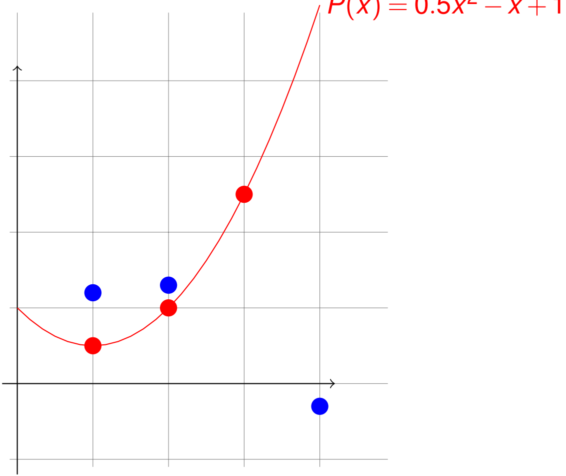
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



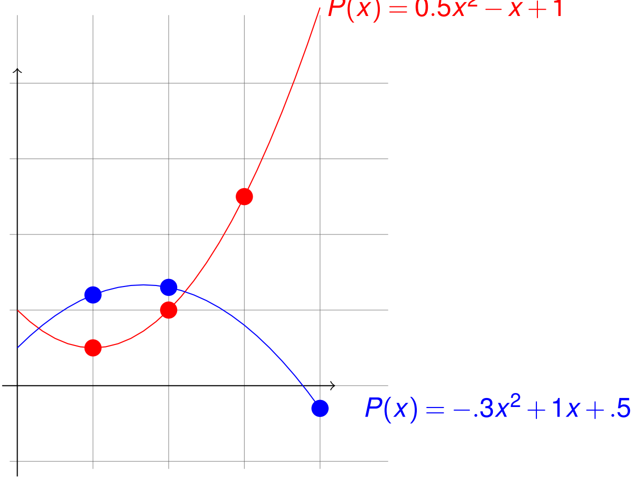
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



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

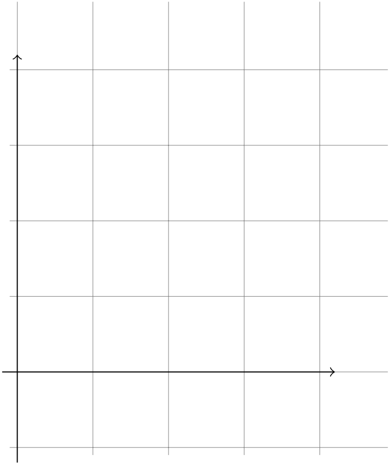
3 points determine a parabola.



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

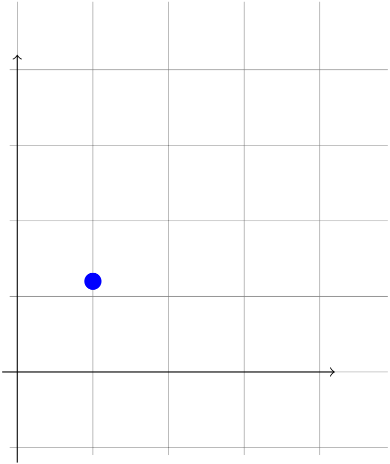
[3] Points with different x values.

2 points not enough.



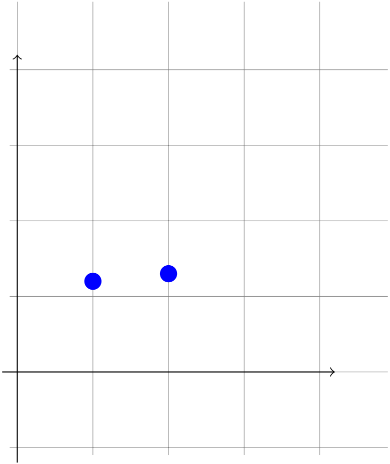
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



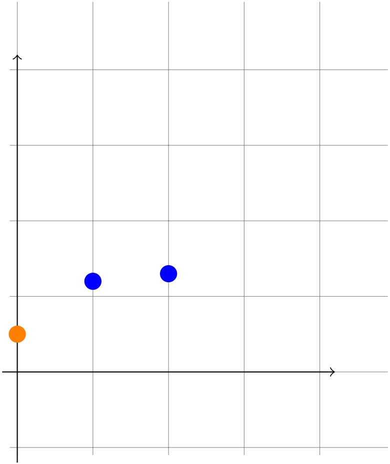
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



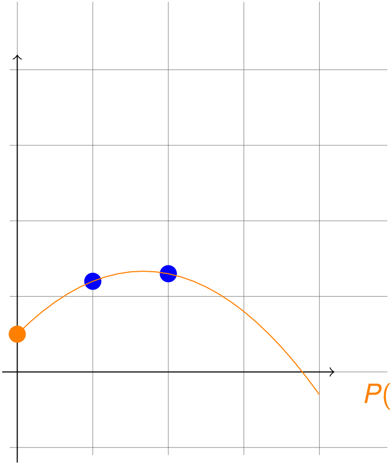
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



There is $P(x)$ contains blue points and *any* $(0, y)$!

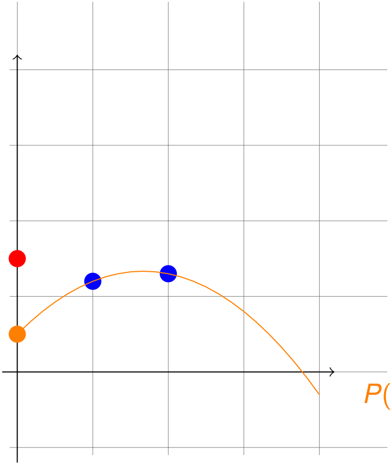
2 points not enough.



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

There is $P(x)$ contains blue points and *any* $(0, y)$!

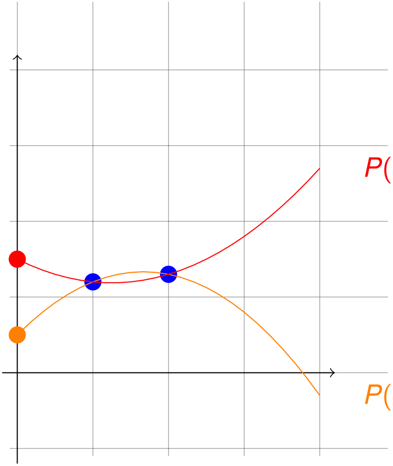
2 points not enough.



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

There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.

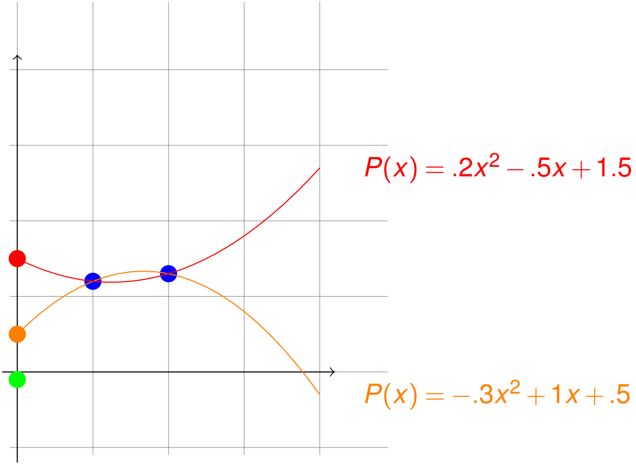


$P(x) = .2x^2 - .5x + 1.5$

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

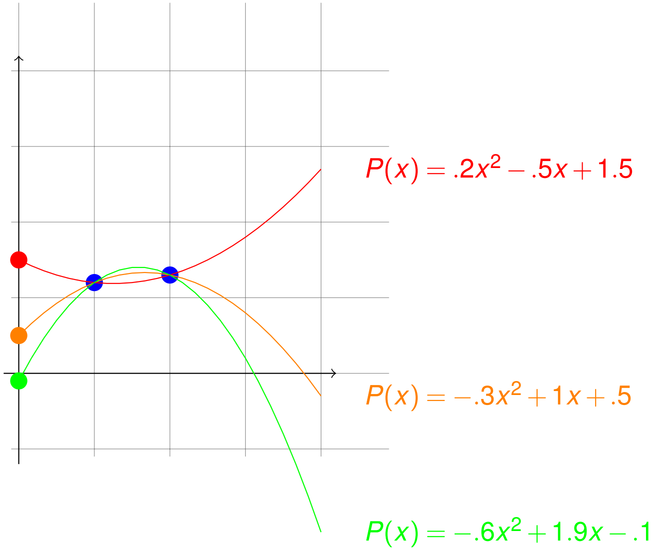
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.

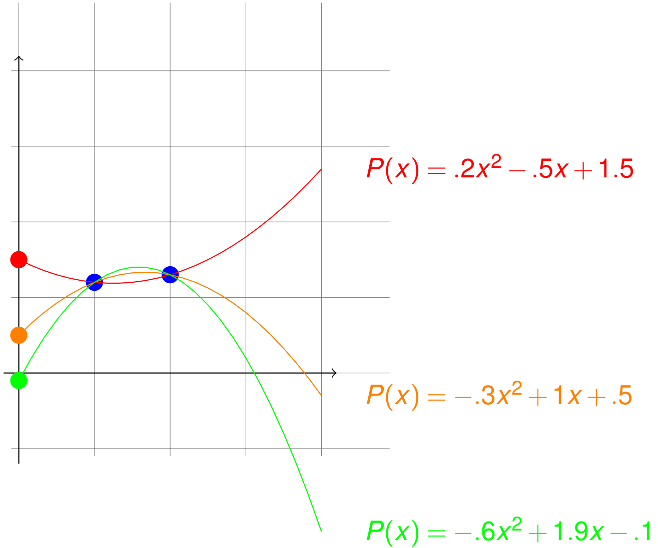


There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



2 points not enough.



There is $P(x)$ contains blue points and *any* $(0, y)$!

Modular Arithmetic Fact and Secrets

Modular Arithmetic Fact and Secrets

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

Modular Arithmetic Fact and Secrets

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

Shamir's k out of n Scheme:

Modular Arithmetic Fact and Secrets

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

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

Modular Arithmetic Fact and Secrets

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

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

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

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $a_0 = s$.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts $\implies$ only one $P(x)$

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.
Knowing $\leq k-1$ pts

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.
Knowing $\leq k-1$ pts $\implies$ any $P(0)$ is possible.

Modular Arithmetic Fact and Secrets

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

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

1. Choose $a_0 = s$, and 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 $(i, P(i) \mod p)$.

Roubustness: Any k shares gives secret.
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.
Knowing $\leq k-1$ pts $\implies$ any $P(0)$ is possible.

What’s my secret?

Remember:
Secret: number from 0 to 10.

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!

What's my secret?

Remember:

Secret: number from 0 to 10.

Any one of you knows nothing!

Any two of you can figure it out!

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!
  Any two of you can figure it out!

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!
  Any two of you can figure it out!

Shares: points on a line.

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!
  Any two of you can figure it out!

Shares: points on a line.
Secret: y-intercept.

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!
  Any two of you can figure it out!

Shares: points on a line.
Secret: y-intercept.
Arithmetic Modulo 11.

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!
  Any two of you can figure it out!

Shares: points on a line.
Secret: y-intercept.
Arithmetic Modulo 11.

What's my secret?

Remember:
Secret: number from 0 to 10.
  Any one of you knows nothing!
  Any two of you can figure it out!

Shares: points on a line.
Secret: y-intercept.
Arithmetic Modulo 11.

What's my secret?

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

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

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

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

$$P(1) = m(1)+b \equiv m+b \equiv 3 \pmod 5$$
$$P(2) = m(2)+b \equiv 2m+b \equiv 4 \pmod 5$$

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

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

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

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

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

$$P(1) = m(1) + b \equiv m + b \equiv 3 \pmod 5$$
$$P(2) = m(2) + b \equiv 2m + b \equiv 4 \pmod 5$$

Subtract first from second..

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

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

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

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, $a_1x+a_0 = mx+b$ 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: $b \equiv 2 \pmod 5$.

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...

$$x + 2 \mod 5.$$

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of $2 \pmod{11}$ is 6:

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of $2 \pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of 2 $\pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$
Multiply both sides by 6.

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of 2 $\pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$
Multiply both sides by 6.

$$12m = 24 \pmod{11}$$

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of 2 $\pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$
Multiply both sides by 6.

$$12m = 24 \pmod{11}$$
$$m = 2 \pmod{11}$$

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of 2 $\pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$
Multiply both sides by 6.

$$12m = 24 \pmod{11}$$
$$m = 2 \pmod{11}$$

Backsolve: $2 + b \equiv 5 \pmod{11}$.

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of $2 \pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$
Multiply both sides by 6.

$$12m = 24 \pmod{11}$$
$$m = 2 \pmod{11}$$

Backsolve: $2 + b \equiv 5 \pmod{11}$. Or $\quad b = 3 \pmod{11}$.

What's my secret?

$$P(1) = m(1) + b \equiv 5 \pmod{11}$$
$$P(3) = m(3) + b \equiv 9 \pmod{11}$$

Subtract first from second.

$$2m \equiv 4 \pmod{11}$$

Multiplicative inverse of $2 \pmod{11}$ is 6: $6 \times 2 \equiv 12 \equiv 1 \pmod{11}$
Multiply both sides by 6.

$$12m = 24 \pmod{11}$$
$$m = 2 \pmod{11}$$

Backsolve: $2 + b \equiv 5 \pmod{11}$. Or $\quad b = 3 \pmod{11}$.

Secret is 3.

Quadratic

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

Quadratic

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

Quadratic

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

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

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: Linear System.

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

In general: Linear System.

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

Solve...

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

In general: Linear System.

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: Linear System.

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: Linear System.

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: Linear System.

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

Another Construction: Interpolation!

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

Another Construction: 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: 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: 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: 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.

Another Construction: 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: 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"

Another Construction: 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.

Another Construction: 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: 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: 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: 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: 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: 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: 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: 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: 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: 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!

Interpolation: in general.

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

Interpolation: in general.

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

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

Interpolation: 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 $x_j \neq x_i$.

Interpolation: 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.

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

Interpolation: 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..

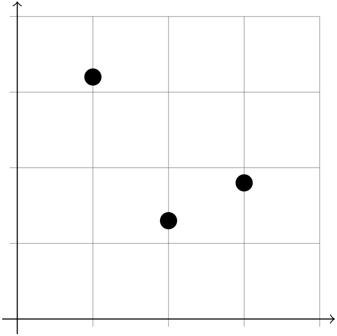
$$P(x) = y_1\Delta_1(x) + y_2\Delta_2(x) + \cdots + y_k\Delta_k(x).$$

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

Construction proves the existence of a degree d polynomial!

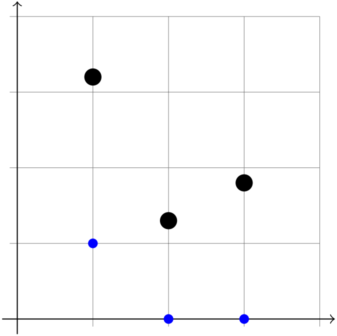
Interpolation: in pictures.

Points: $(1, 3.2)$, $(2, 1.3)$, $(3, 1.8)$.



Interpolation: in pictures.

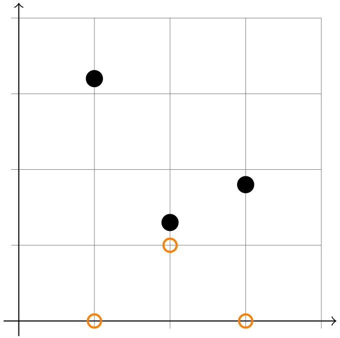
Points: $(1,3.2)$, $(2,1.3)$, $(3,1.8)$.



$\Delta_1(x)$

Interpolation: in pictures.

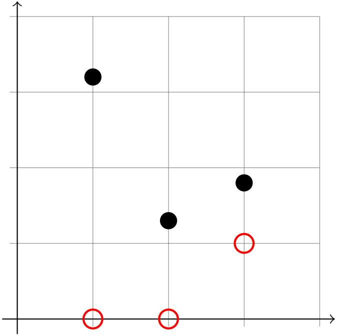
Points: $(1, 3.2)$, $(2, 1.3)$, $(3, 1.8)$.



$\Delta_1(x)$ $\Delta_2(x)$

Interpolation: in pictures.

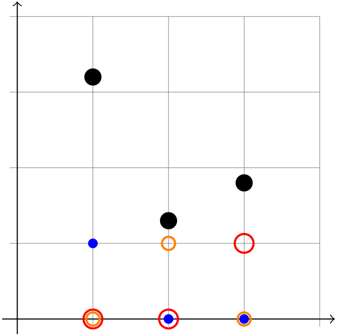
Points: $(1, 3.2)$, $(2, 1.3)$, $(3, 1.8)$.



$\Delta_1(x)$ $\Delta_2(x)$ $\Delta_3(x)$

Interpolation: in pictures.

Points: $(1, 3.2)$, $(2, 1.3)$, $(3, 1.8)$.

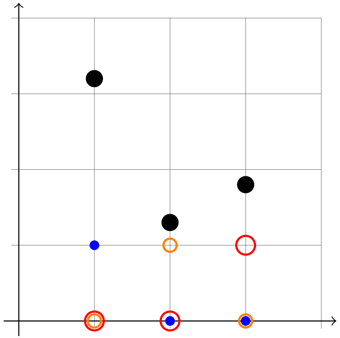


$\Delta_1(x)$ $\Delta_2(x)$ $\Delta_3(x)$

Scale each Δ_i function and add to contain points.

Interpolation: in pictures.

Points: $(1, 3.2)$, $(2, 1.3)$, $(3, 1.8)$.



$\Delta_1(x)$ $\Delta_2(x)$ $\Delta_3(x)$

Scale each Δ_i function and add to contain points.

$$P(x) = 3.2\ \Delta_1(x) + 1.3\Delta_2(x) + 1.8\Delta_3(x)$$

Interpolation and Existence

Interpolation takes $d+1$ points and produces a degree d polynomial that contains the points.

Interpolation and Existence

Interpolation takes $d+1$ points and produces a degree d polynomial that contains the points.

Construction proves the existence of a degree d polynomial that contains points!

Interpolation and Existence

Interpolation takes $d+1$ points and produces a degree d polynomial that contains the points.

Construction proves the existence of a degree d polynomial that contains points!

Is it the only degree d polynomial that contains the points?

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 - 2 x)
```

Polynomial Division.

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

```
                   4 x + 4
          -----------------
x - 3 ) 4x^2 - 3 x + 2
     - (4x^2 - 2 x)
        ----------
                   4 x + 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 - 2 x)
        ----------
                4 x + 2
             - (4 x - 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 - 2 x)
        ----------
                4 x + 2
             - (4 x - 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 - 2 x)
        ----------
               4 x + 2
          - (4 x - 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 - 2 x)
            ----------
                4 x + 2
             - (4 x - 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 - 2 x)
        ----------
               4 x + 2
            - (4 x - 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 - 2 x)
        ----------
              4 x + 2
           - (4 x - 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 $r = 0$. □

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.

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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.

Only d roots.

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

Proof: $P(x) = (x-a)Q(x) + r$.
Plugin a: $P(a) = r$. It is a root if and only if $r = 0$. □

Lemma 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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.

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; $r_1, \dots, r_d$ 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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.
Root either at r_1 or root of $Q(x)$.

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: $P(a) = r$. 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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.
Root either at r_1 or root of $Q(x)$.

$Q(x)$ has smaller degree and $r_2, \ldots r_d$ are roots.

Only d roots.

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

Proof: $P(x) = (x-a)Q(x) + r$.
Plugin a: $P(a) = r$. It is a root if and only if $r = 0$. □

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

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

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.
Root either at r_1 or root of $Q(x)$.

$Q(x)$ has smaller degree and $r_2, \ldots r_d$ are roots.
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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.
Root either at r_1 or root of $Q(x)$.

$Q(x)$ has smaller degree and $r_2, \ldots r_d$ are roots.
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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.
Root either at r_1 or root of $Q(x)$.

$Q(x)$ has smaller degree and $r_2, \ldots r_d$ are roots.
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.

$P(x) = 0$ if and only if $(x-r_1)$ is 0 or $Q(x) = 0$.
$ab = 0 \implies a = 0$ or $b = 0$ in field.
Root either at r_1 or root of $Q(x)$.

$Q(x)$ has smaller degree and $r_2, \ldots r_d$ are roots.
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.