Introduction

Introduction

Co Teacher: Professor Jean Walrand.

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).
Research in Probability as well.

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).
Research in Probability as well.

Email: walrand@berkeley.edu

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).
Research in Probability as well.

Email: walrand@berkeley.edu
Office Hours: 257 Cory Hall

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).
Research in Probability as well.

Email: walrand@berkeley.edu
Office Hours: 257 Cory Hall
2:30-3:30 Monday

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).
Research in Probability as well.

Email: walrand@berkeley.edu
Office Hours: 257 Cory Hall
2:30-3:30 Monday
2:30-3:30 Wednesday

Introduction

Co Teacher: Professor Jean Walrand.

Will begin lecturer in mid October.

Lectures on Probabilty.
Teaches Probability (EE 126,...).
Research in Probability as well.

Email: walrand@berkeley.edu
Office Hours: 257 Cory Hall
2:30-3:30 Monday
2:30-3:30 Wednesday

Jean Walrand – Prof. of EECS – UCB
257 Cory Hall – walrand@berkeley.edu

I was born in Belgium(1) and came to Berkeley for my PhD. I have been teaching at UCB since 1982.

My wife and I live in Berkeley. We have two daughters (UC alumni – Go Bears!). We like to ski and play tennis (both poorly). We enjoy classical music and jazz.

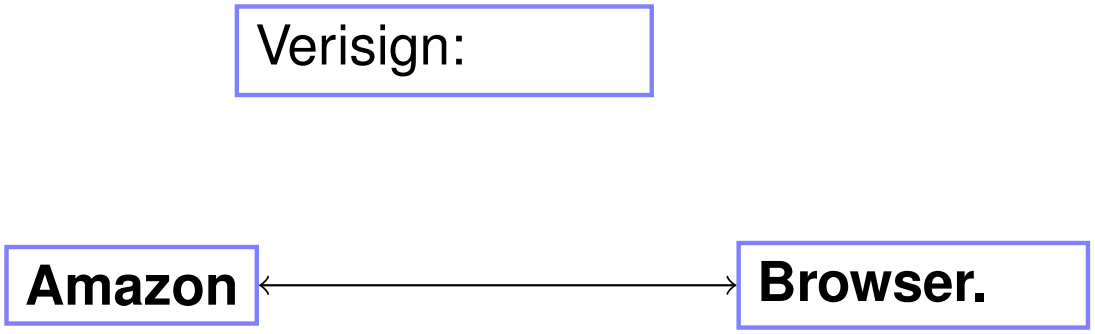
My research interests include stochastic systems, networks and game theory.

(1)

Lecture 13. Outline.

1. Signature Schemes
2. Polynomials
3. Secret Sharing
4. Polynomial Interpolation

Signatures using RSA.



Signatures using RSA.

Verisign:

Amazon ⟷ **Browser.**

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Signatures using RSA.

Verisign: k_V, K_V

Amazon $\longleftrightarrow$ **Browser.**

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Signatures using RSA.

Verisign: k_V, K_V

Amazon $\longleftrightarrow$ **Browser.** K_V

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Signatures using RSA.

Verisign: k_V, K_V

Amazon $\longleftrightarrow$ **Browser.** K_V

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Signatures using RSA.

Verisign: k_v, K_v

$[C, S_v(C)]$

Amazon $\longleftrightarrow$ **Browser.** K_v

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

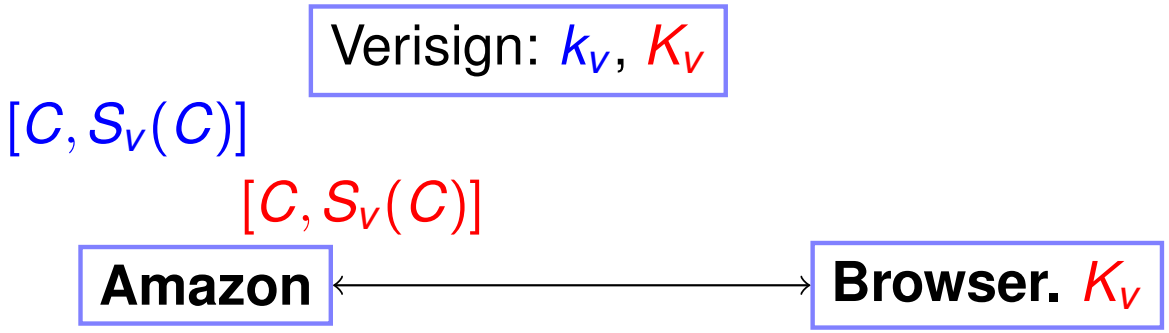
Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Signatures using RSA.



Certificate Authority: Verisign, GoDaddy, DigiNotar,...

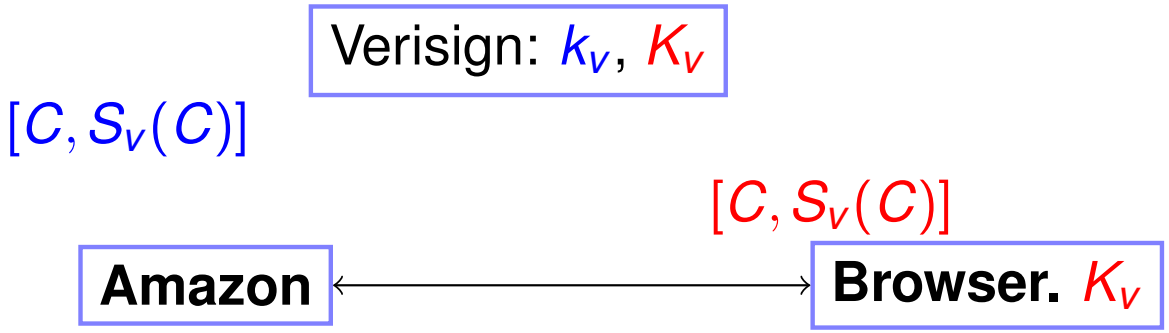
Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Signatures using RSA.



Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

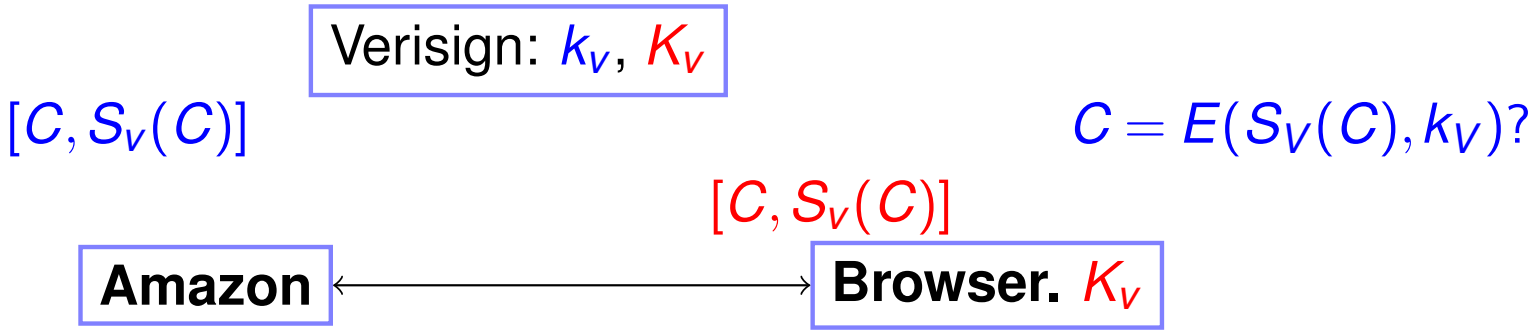
Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Signatures using RSA.



Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

Signatures using RSA.

Verisign: k_v, K_v

$[C, S_v(C)]$ $\qquad$ $C = E(S_V(C), k_V)$?

$[C, S_v(C)]$

Amazon $\longleftrightarrow$ **Browser.** K_v

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V)$

Signatures using RSA.

Verisign: k_v, K_v

$[C, S_v(C)]$ $\qquad$ $C = E(S_V(C), k_V)$?

$[C, S_v(C)]$

Amazon $\longleftrightarrow$ **Browser.** K_v

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V) = (S_v(C))^e$

Signatures using RSA.

Verisign: k_v, K_v

$[C, S_v(C)]$ $\qquad\qquad$ $C = E(S_V(C), k_V)$?

$[C, S_v(C)]$

Amazon $\longleftrightarrow$ **Browser.** K_v

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V) = (S_v(C))^e = (C^d)^e$

Signatures using RSA.

Verisign: k_v, K_v

$[C, S_v(C)]$

$C = E(S_V(C), k_V)$?

$[C, S_v(C)]$

Amazon $\longleftrightarrow$ **Browser.** K_v

Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

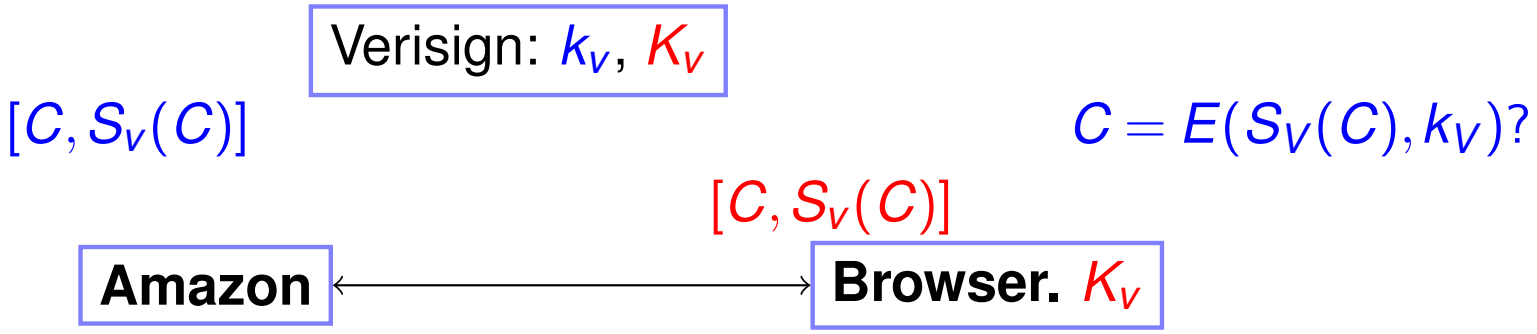
Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V) = (S_v(C))^e = (C^d)^e = C^{de}$

Signatures using RSA.



Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

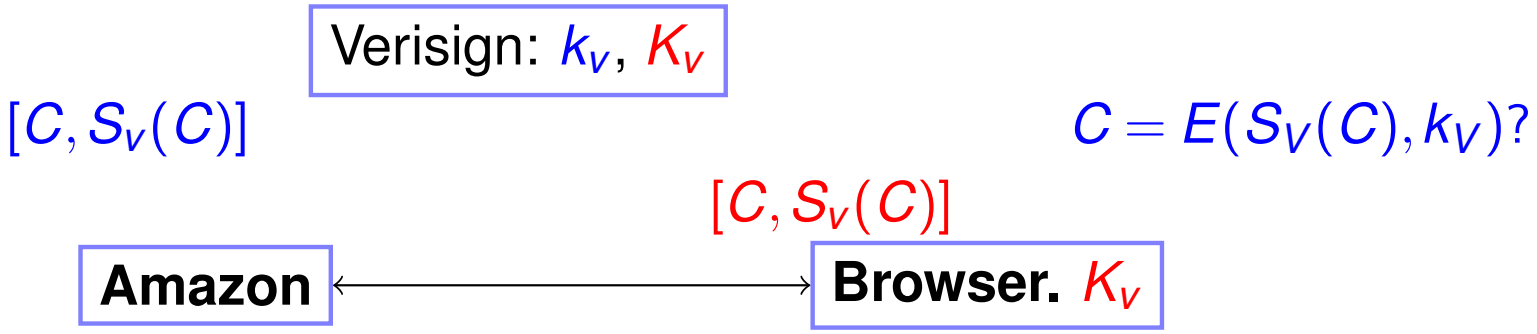
Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V) = (S_v(C))^e = (C^d)^e = C^{de} = C \pmod N$

Signatures using RSA.



Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

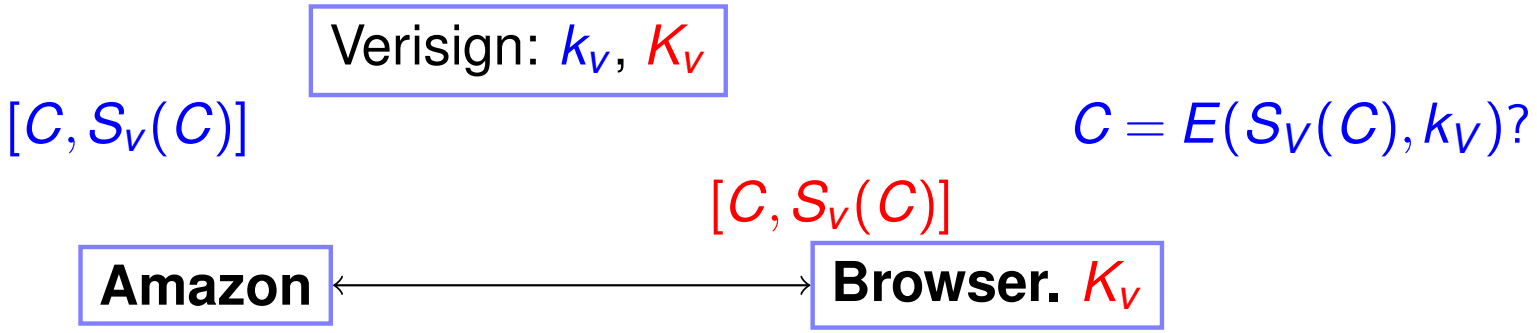
Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V) = (S_v(C))^e = (C^d)^e = C^{de} = C \pmod N$

Valid signature of Amazon certificate C!

Signatures using RSA.



Certificate Authority: Verisign, GoDaddy, DigiNotar,...

Verisign's key: $K_V = (N, e)$ and $k_V = d$ ($N = pq$.)

Browser "knows" Verisign's public key: K_V.

Amazon Certificate: C = "I am Amazon. My public Key is K_A."

Versign signature of C: $S_v(C)$: $D(C, k_V) = C^d \mod N$.

Browser receives: $[C, y]$

Verifies Signature by Verisign: Checks $E(y, K_V) = C$?

$E(S_v(C), K_V) = (S_v(C))^e = (C^d)^e = C^{de} = C \pmod N$
Valid signature of Amazon certificate C!

Security: Eve can't forge unless she "breaks" RSA scheme.

RSA, Public Key, and Signatures.

RSA, Public Key, and Signatures.

RSA:

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

Signature scheme:

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m, K), k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

$E(D(C, k), K) = (C^d)^e \mod N = C$

Other Eve.

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

... and August 28, 2011 announcement.

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

... and August 28, 2011 announcement.

DigiNotar Certificate issued for Microsoft!!!

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

... and August 28, 2011 announcement.

DigiNotar Certificate issued for Microsoft!!!

.... and 2013.

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

... and August 28, 2011 announcement.

DigiNotar Certificate issued for Microsoft!!!

.... and 2013.

TurkTrust issued Google certificate used in attacks.

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

... and August 28, 2011 announcement.

DigiNotar Certificate issued for Microsoft!!!

.... and 2013.

TurkTrust issued Google certificate used in attacks.

How does Microsoft get a CA to issue certificate to them ...

Other Eve.

Get CA to certify fake certificates: Microsoft Corporation.

2001..Doh.

... and August 28, 2011 announcement.

DigiNotar Certificate issued for Microsoft!!!

.... and 2013.

TurkTrust issued Google certificate used in attacks.

How does Microsoft get a CA to issue certificate to them ...

and only them?

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.

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Trivial: $k = 1$.

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Trivial: $k = 1$. Tell everyone the secret!

Secret Sharing.

Share secret among n people.

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

$k=3, n=5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Trivial: $k=1$. Tell everyone the secret!

For $k=2$

Secret Sharing.

Share secret among n people.

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

$k = 3, n = 5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Trivial: $k = 1$. Tell everyone the secret!

For $k = 2$?

Secret Sharing.

Share secret among n people.

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

$k=3, n=5$
Any 3 out of 5 people will know secret.
Any 2 out of 5 people will know nothing!

Trivial: $k=1$. Tell everyone the secret!

For $k=2$? ???

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

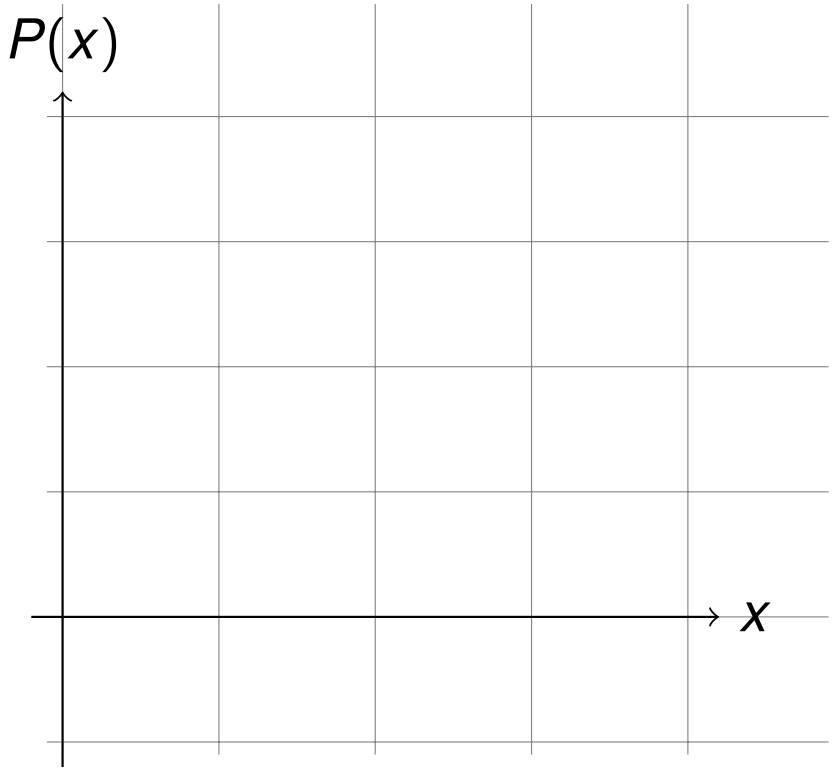
Line:$P(x) = a_1 x + a_0$

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

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

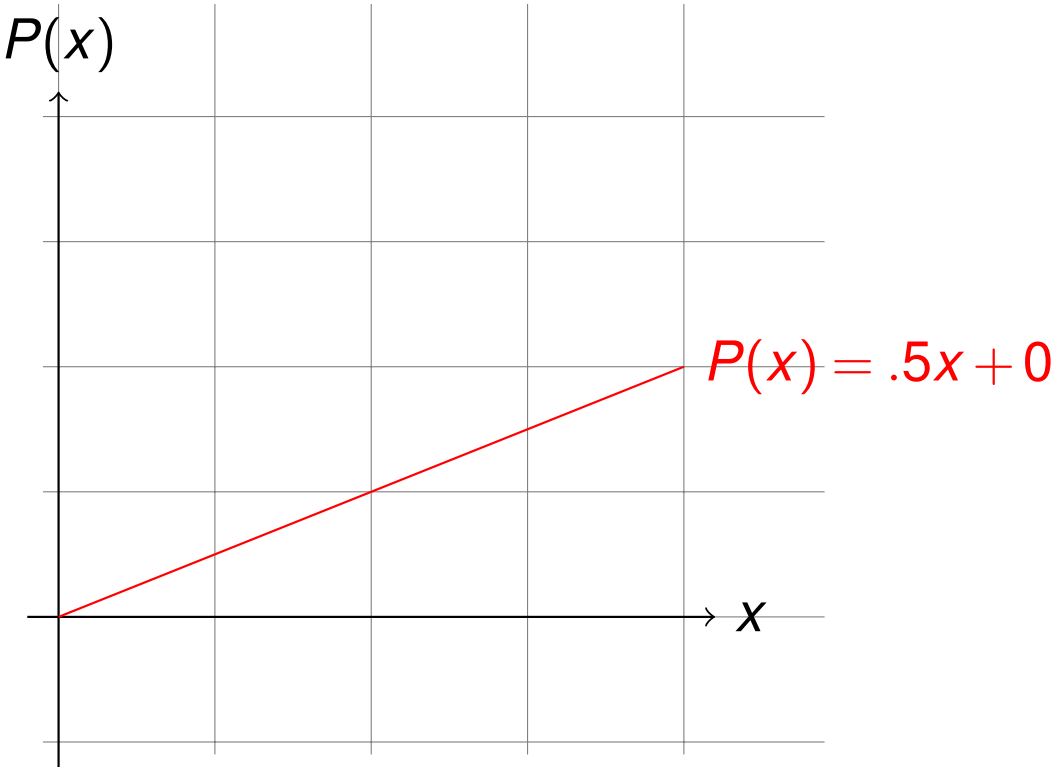
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



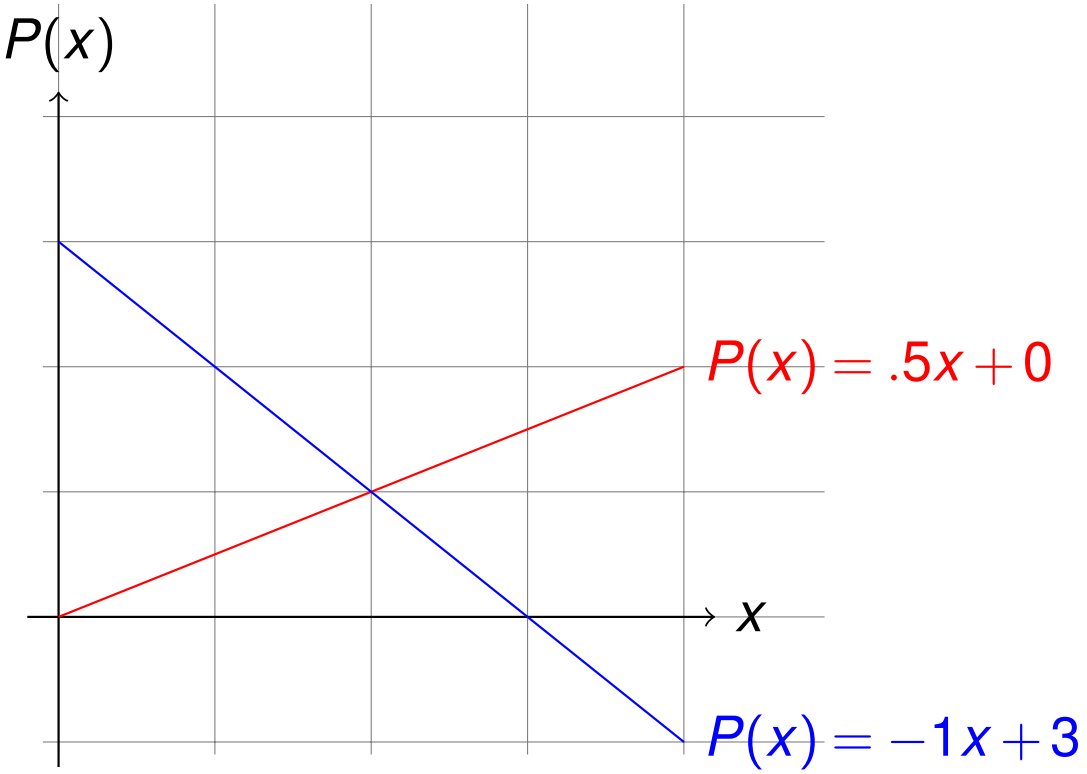
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



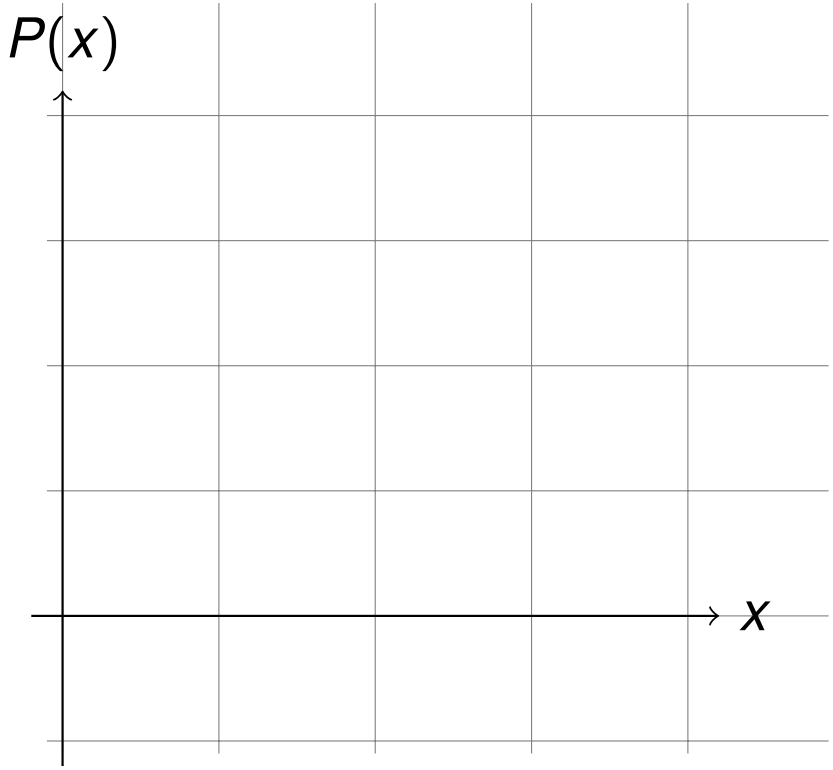
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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



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

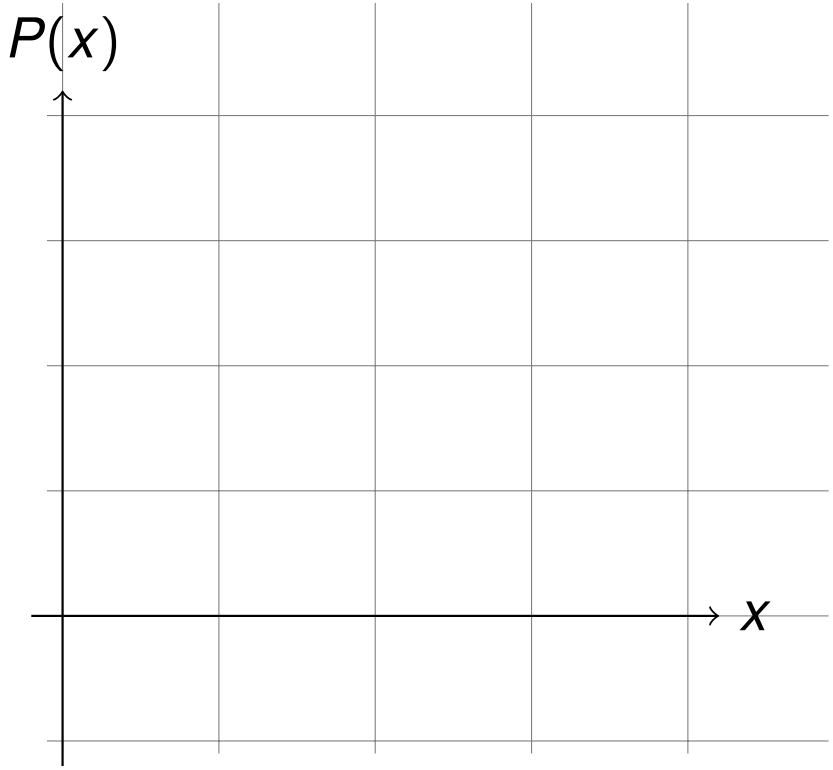
Line: $P(x) = a_1 x + a_0 = mx + b$



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

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

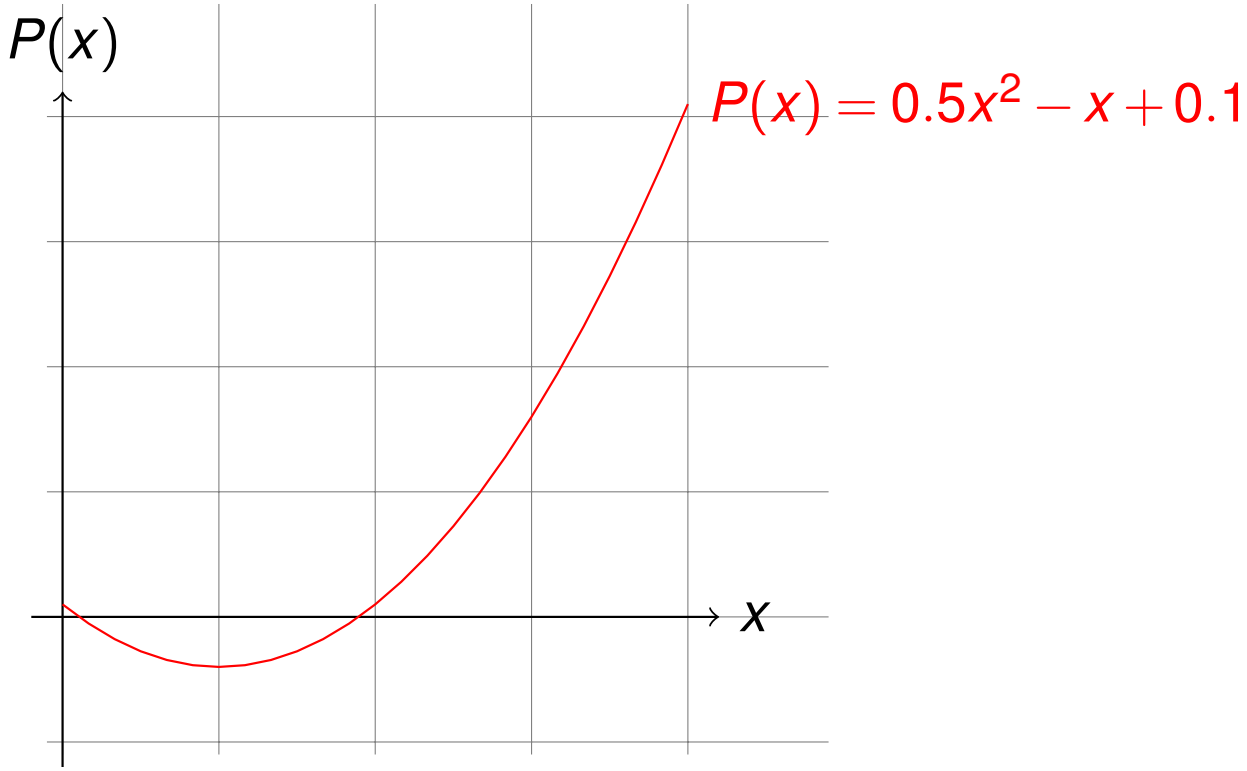
Line: $P(x) = a_1 x + a_0 = mx + b$



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

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

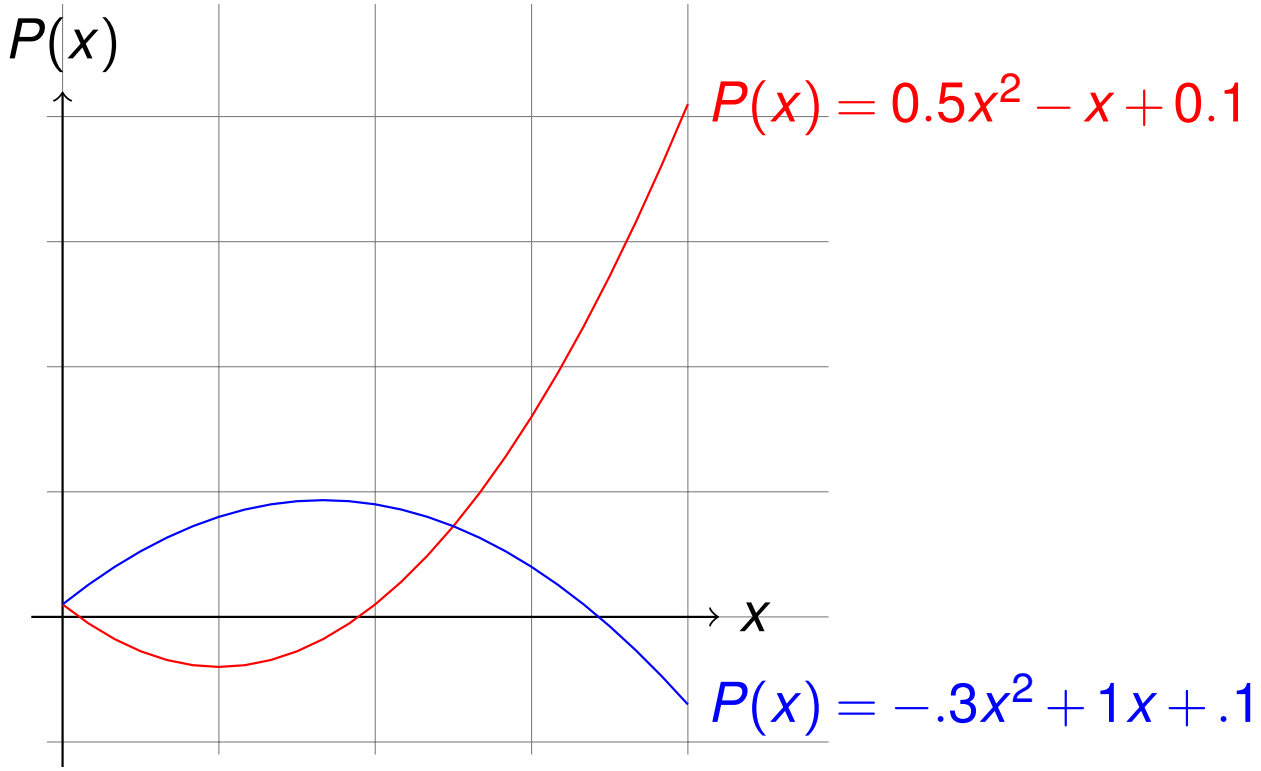
Line: $P(x) = a_1 x + a_0 = mx + b$



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

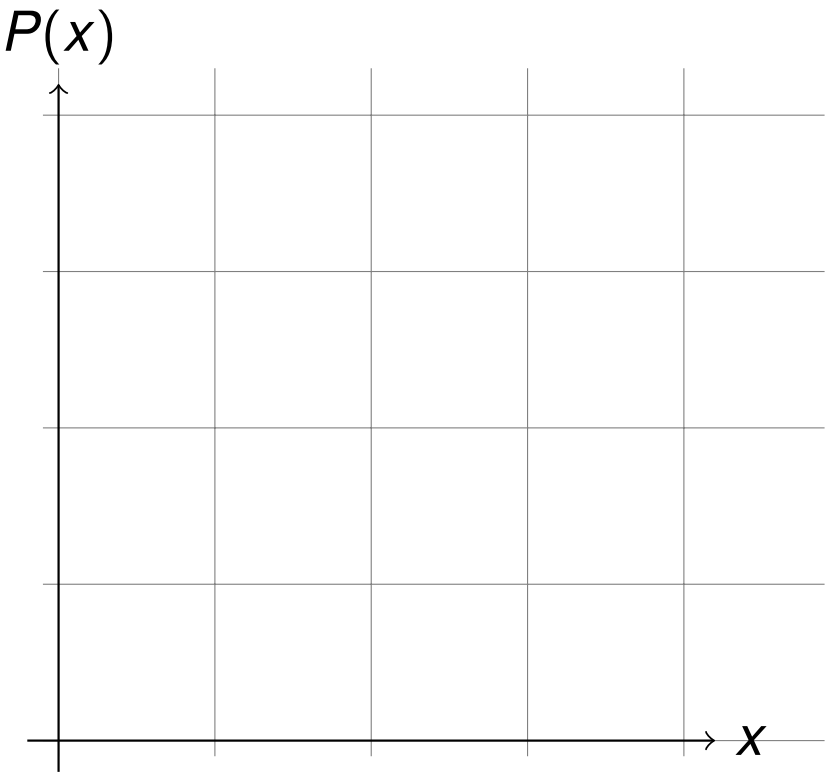
Polynomial: $P(x) = a_d x^4 + \cdots + a_0$

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

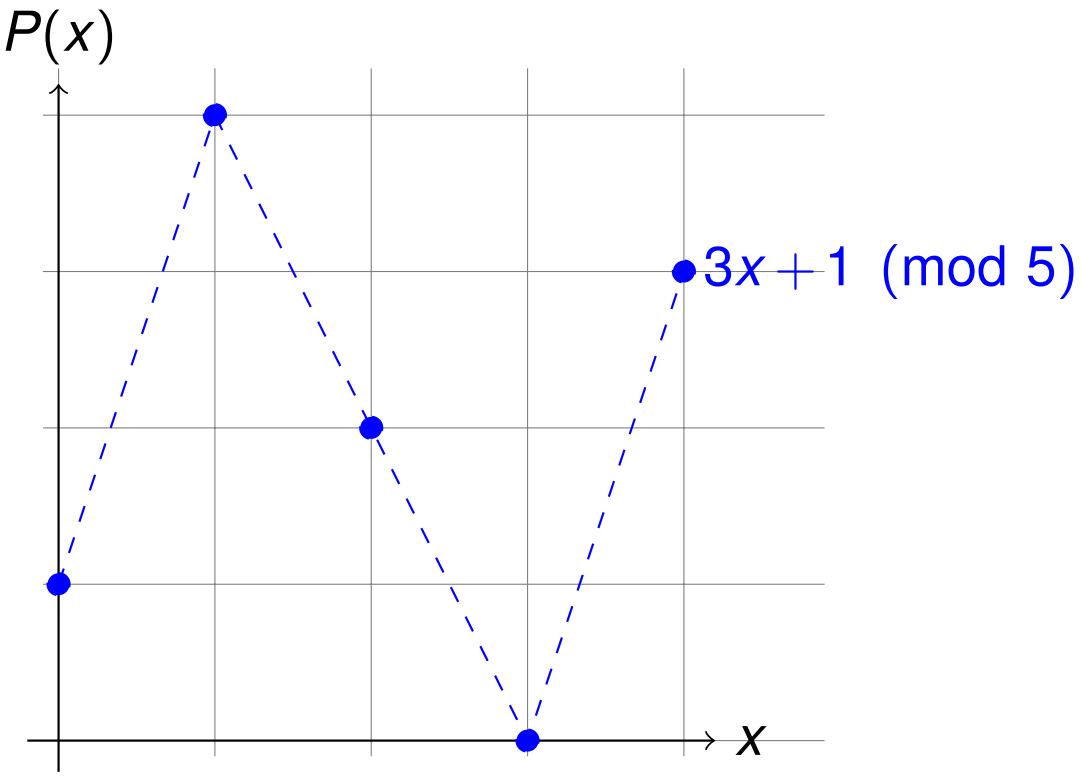


Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

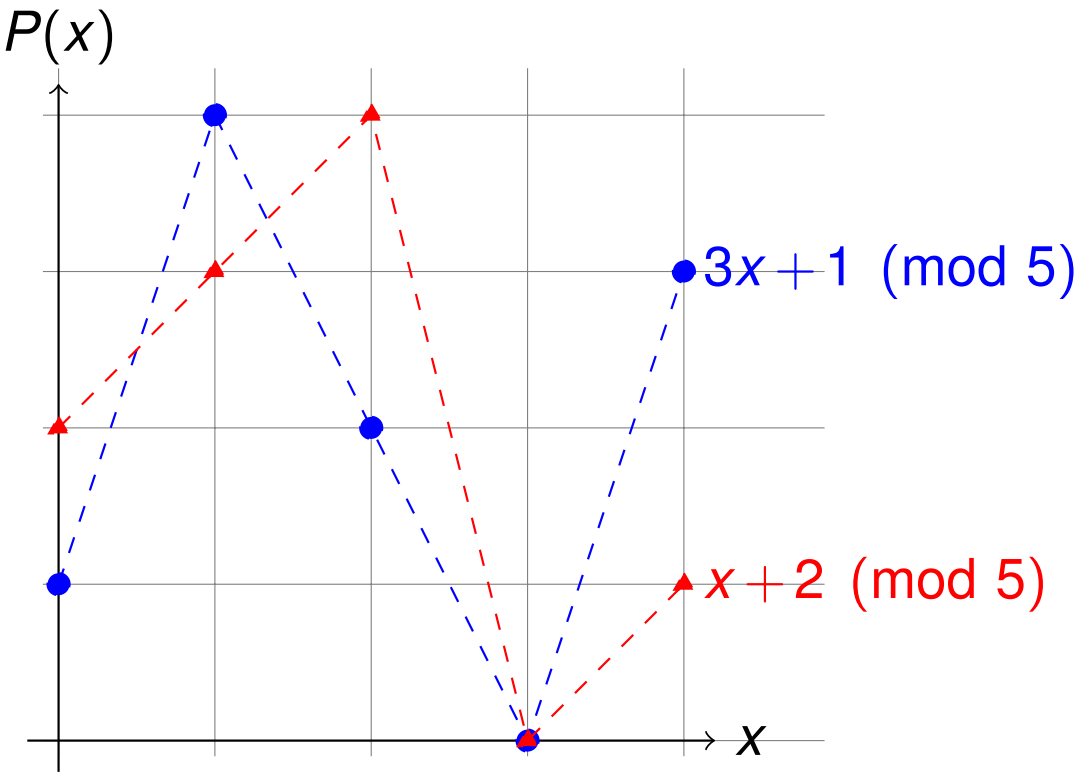
Polynomial: $P(x) = a_d x^4 + \cdots + a_0 \pmod{p}$



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



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

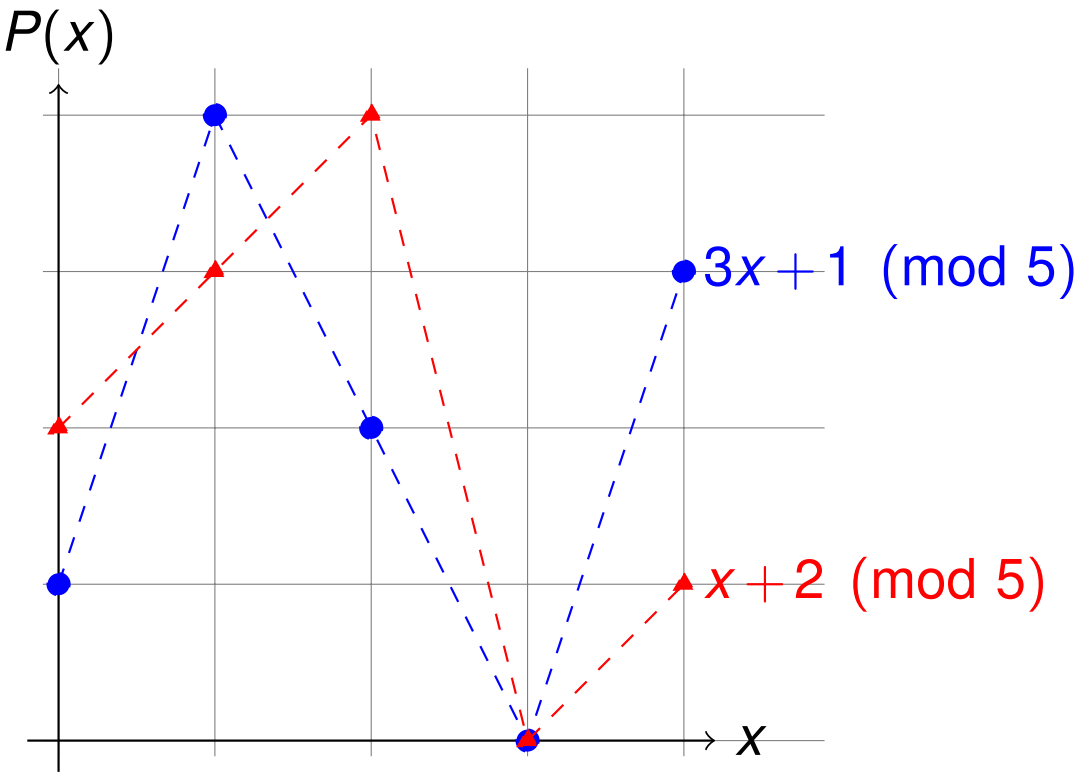


Finding an intersection.

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

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

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



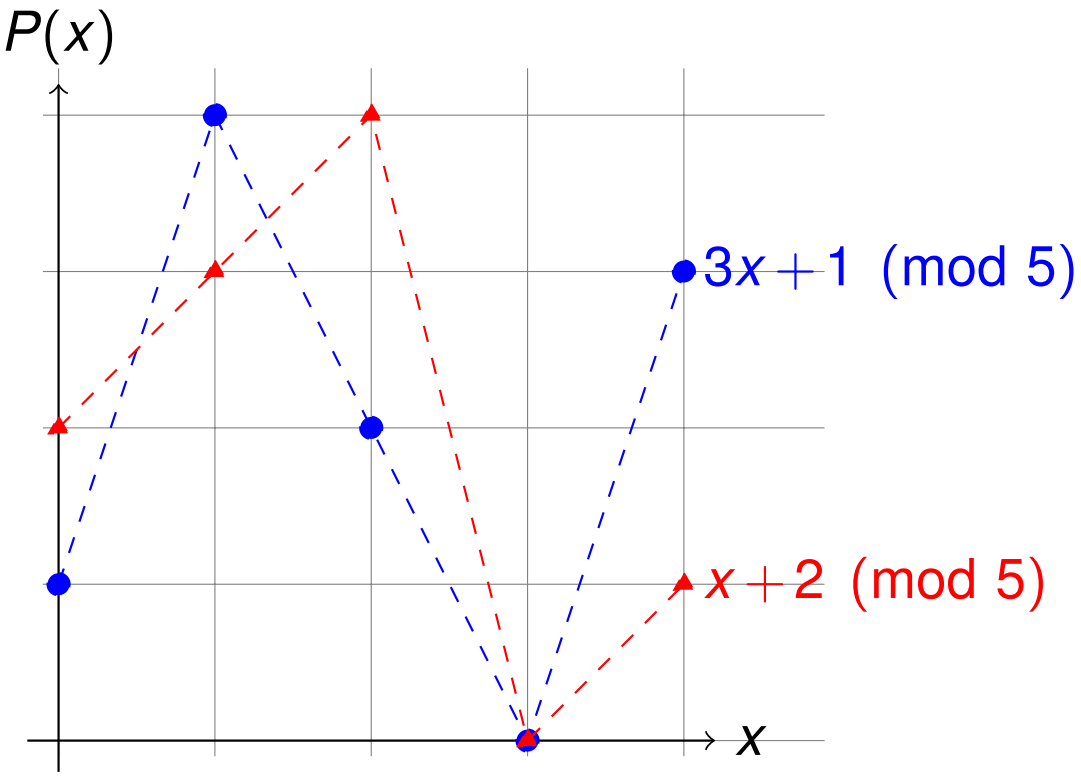
Finding an intersection.

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

$\implies 2x \equiv 1 \pmod 5 \implies x \equiv 3 \pmod 5$

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. Three points specify a parabola.

[2] Points with different x values.

Two points make a line.

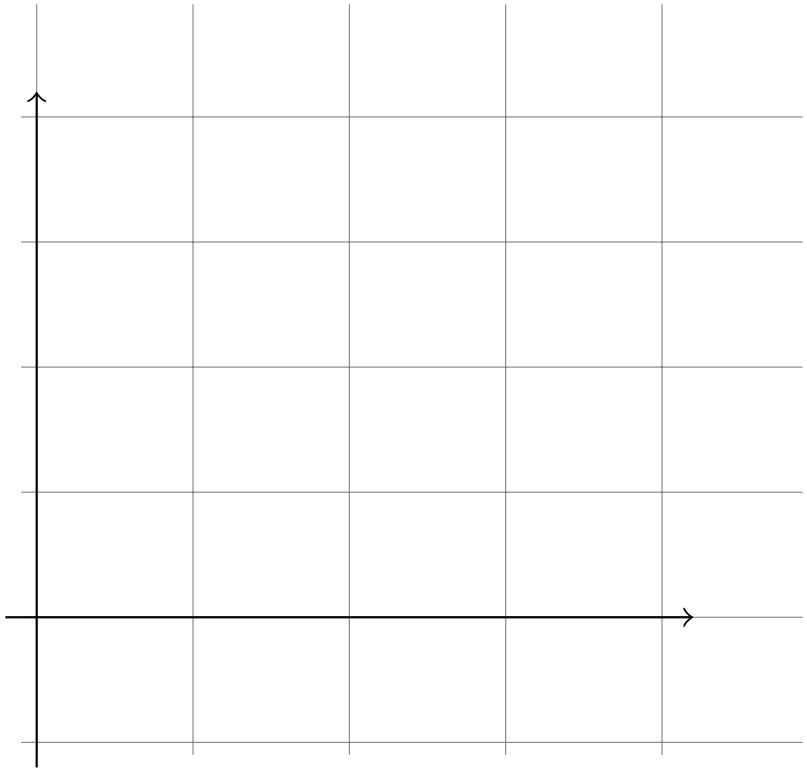
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [2]

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

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

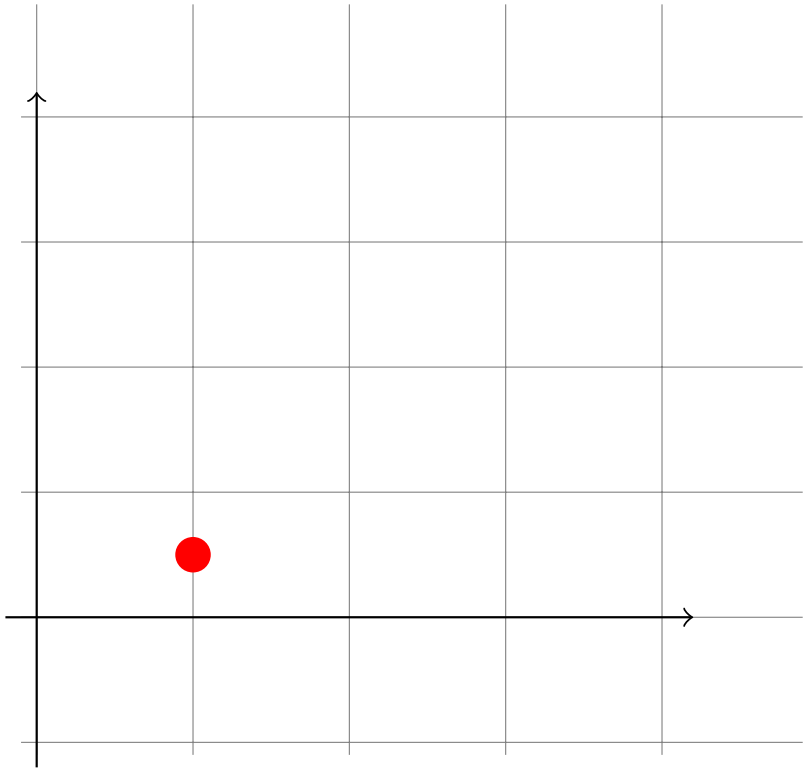
[2] Points with different x values.

3 points determine a parabola.



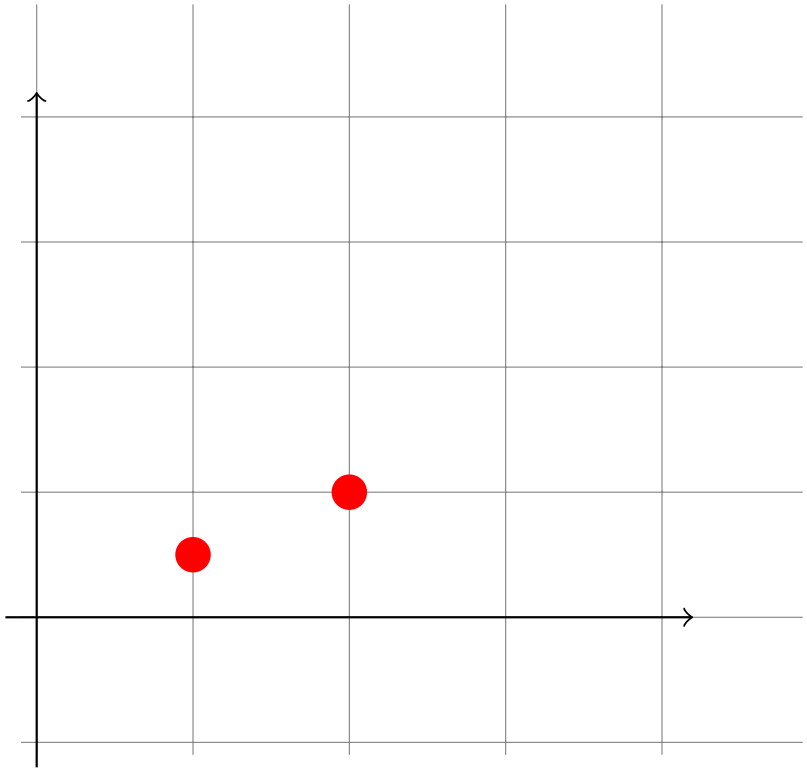
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



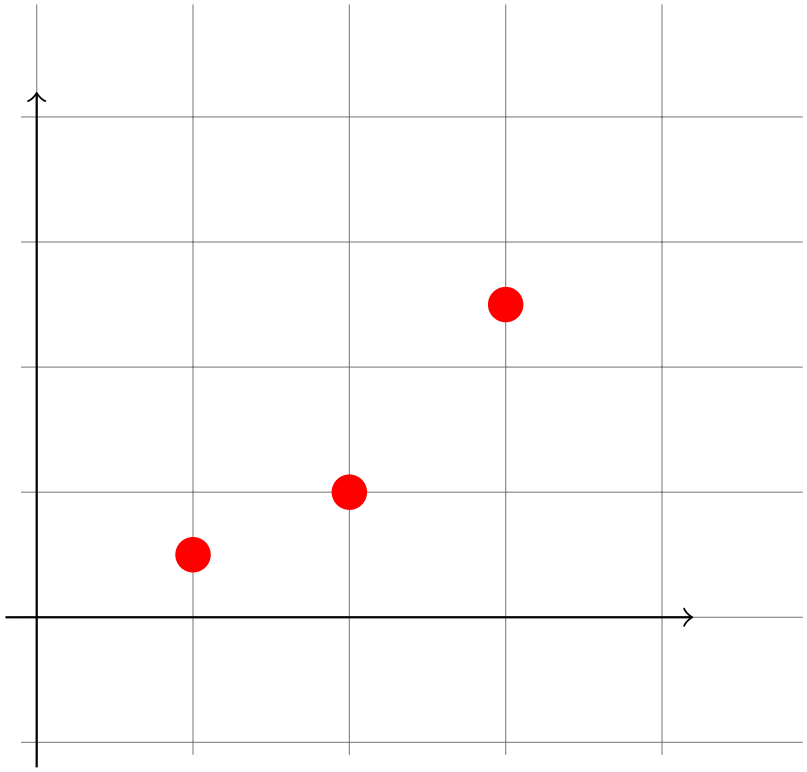
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



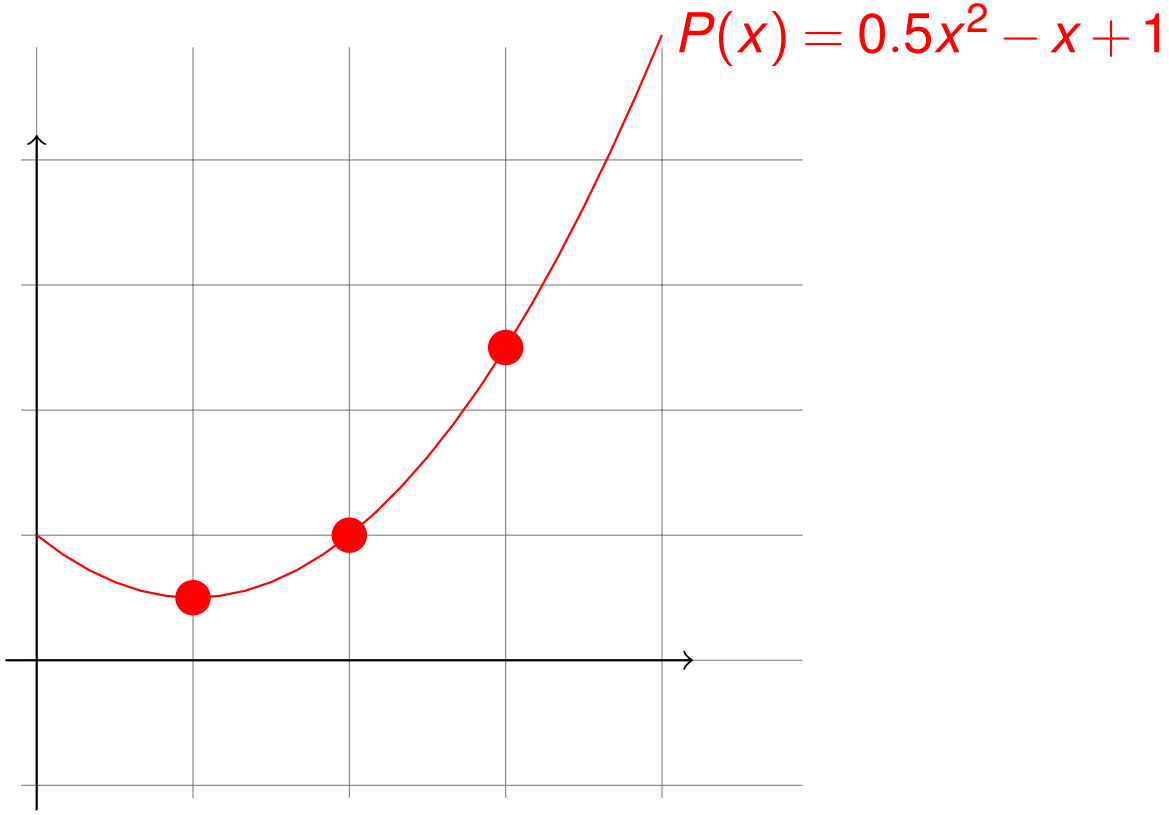
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



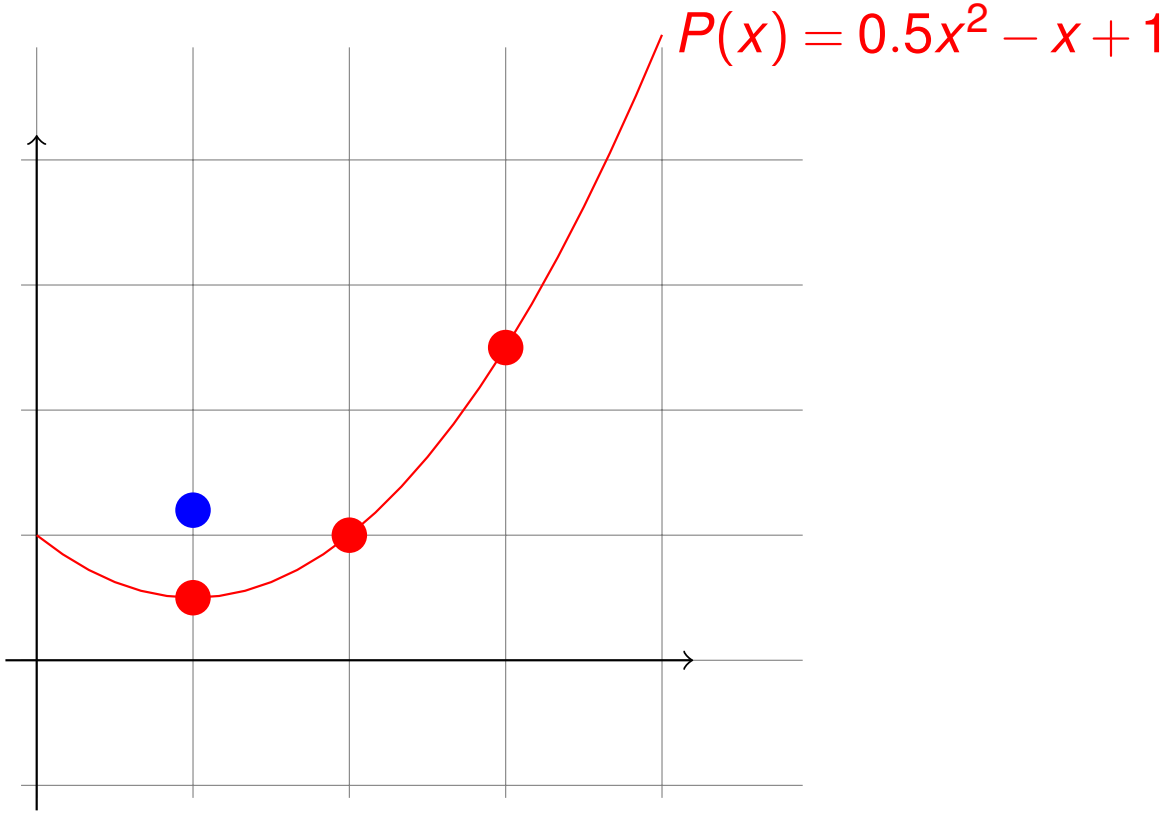
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



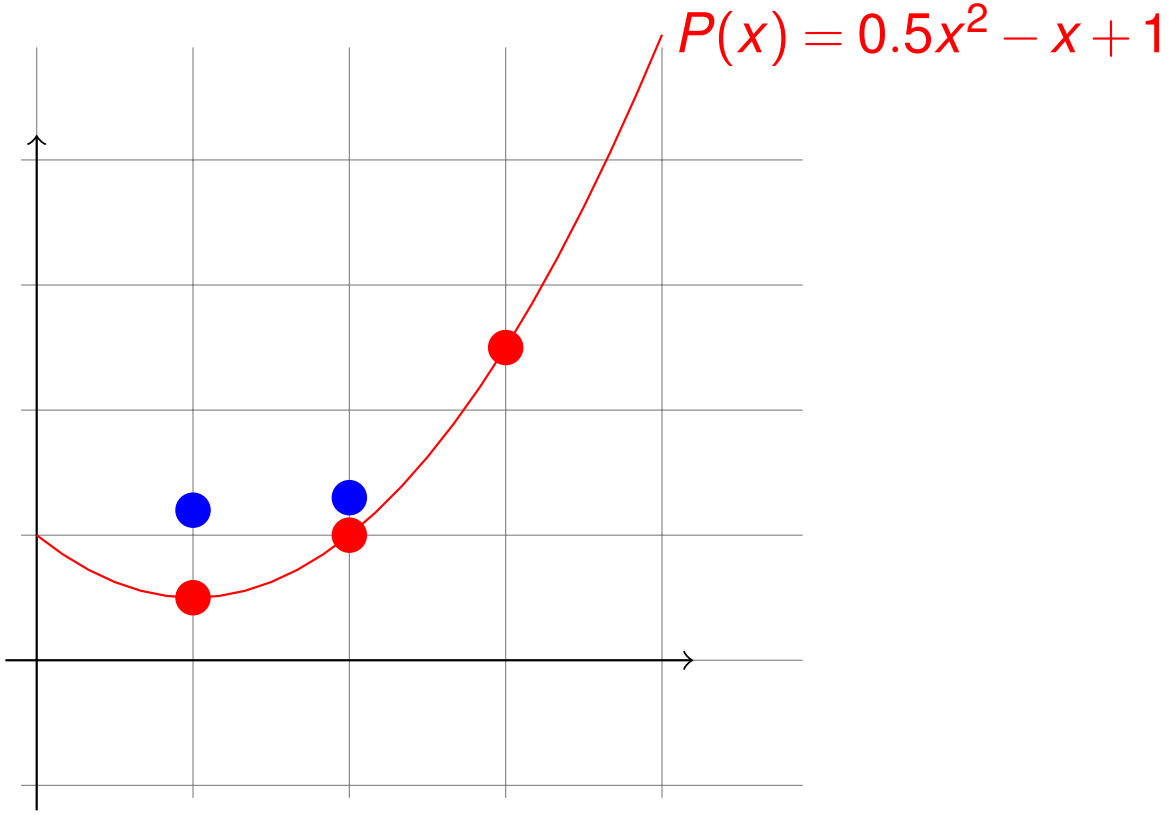
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



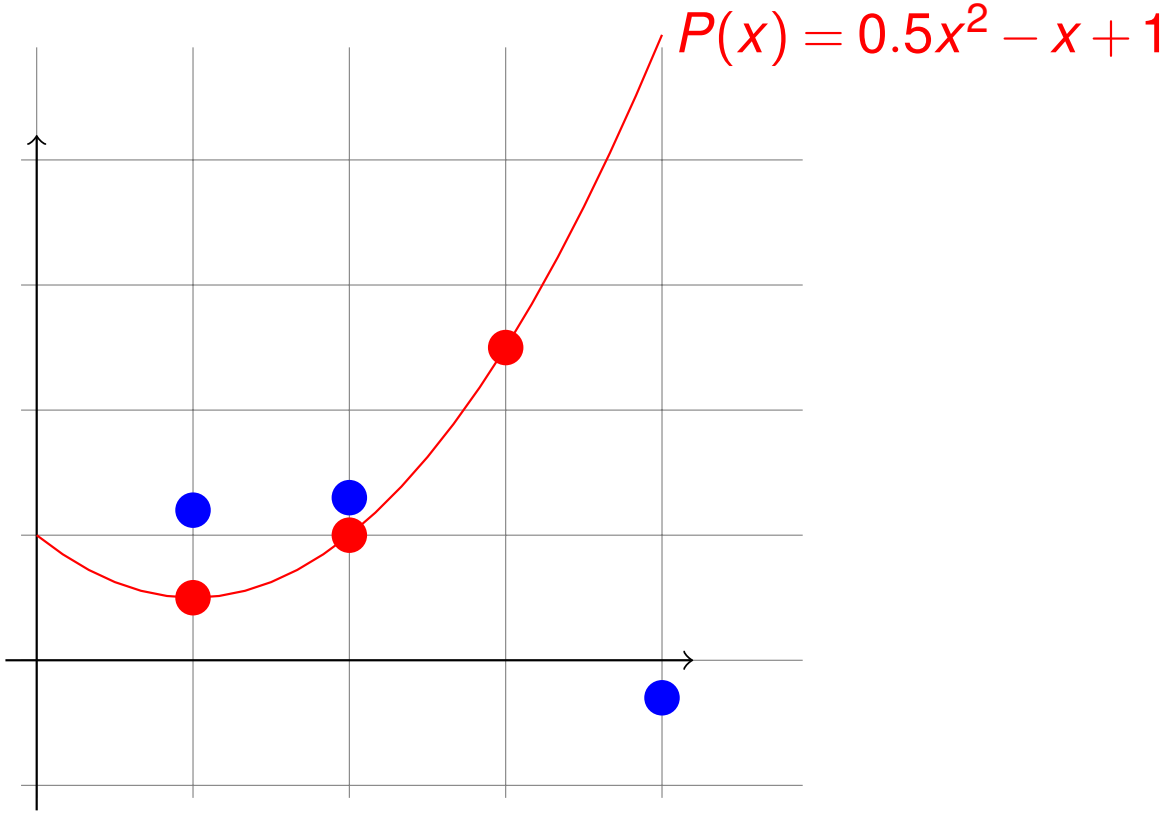
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



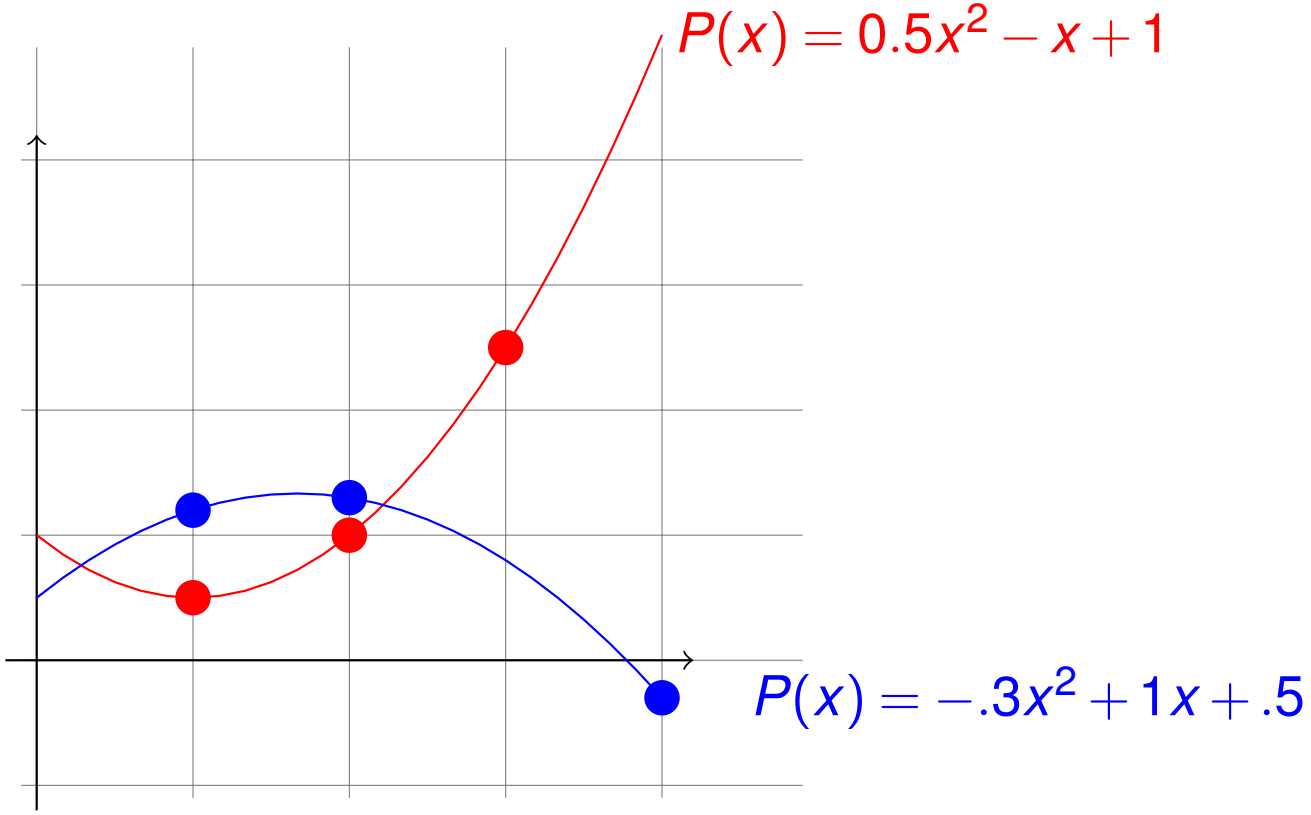
Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

3 points determine a parabola.



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

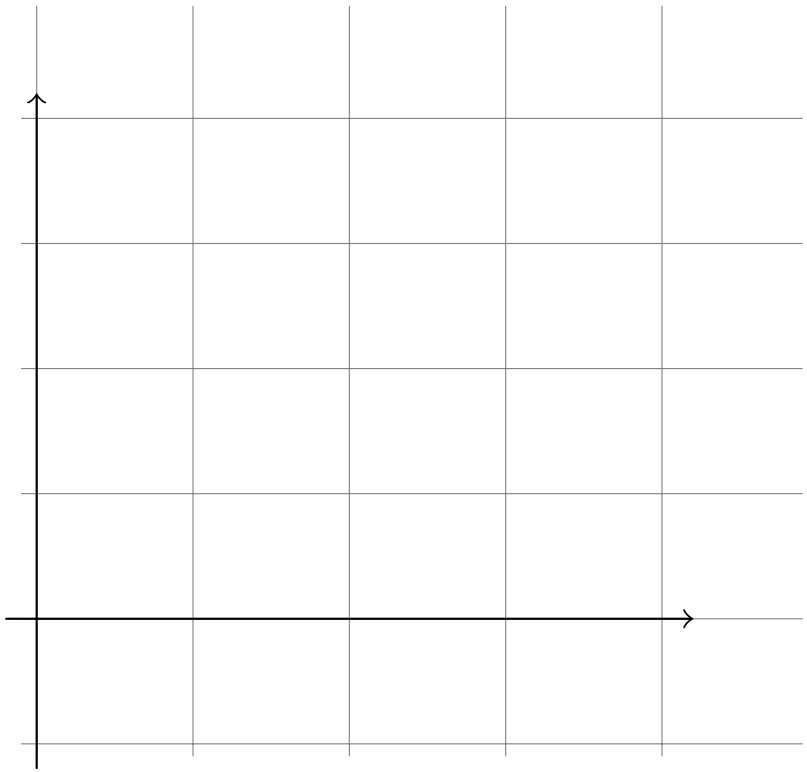
3 points determine a parabola.



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

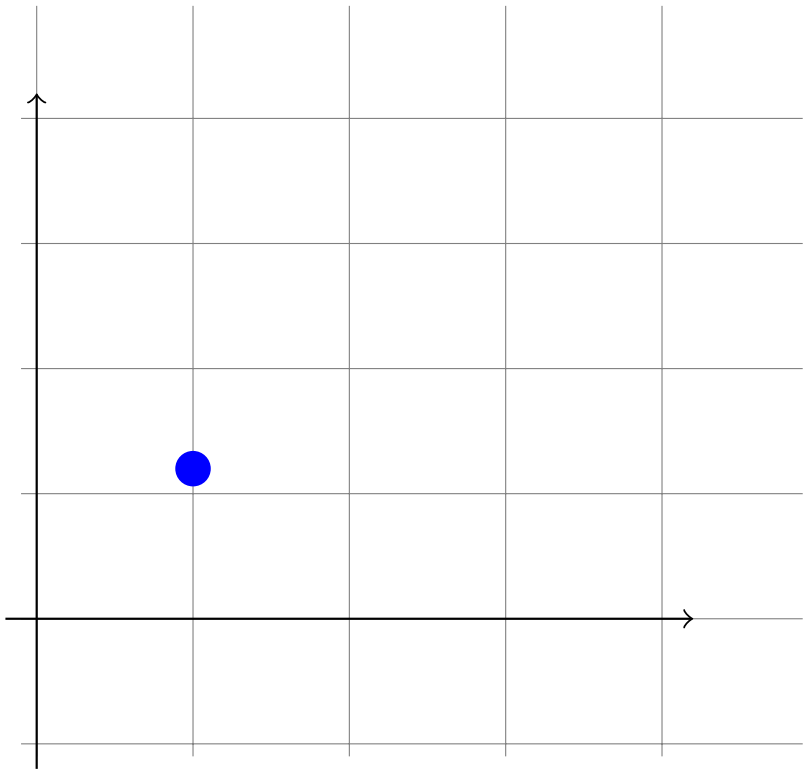
[3] Points with different x values.

2 points not enough.



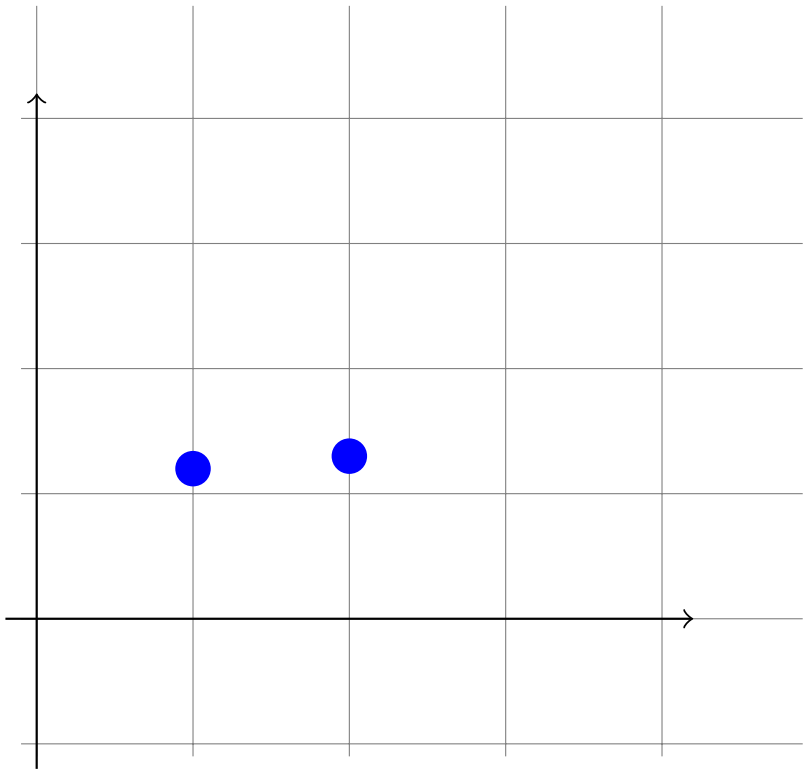
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



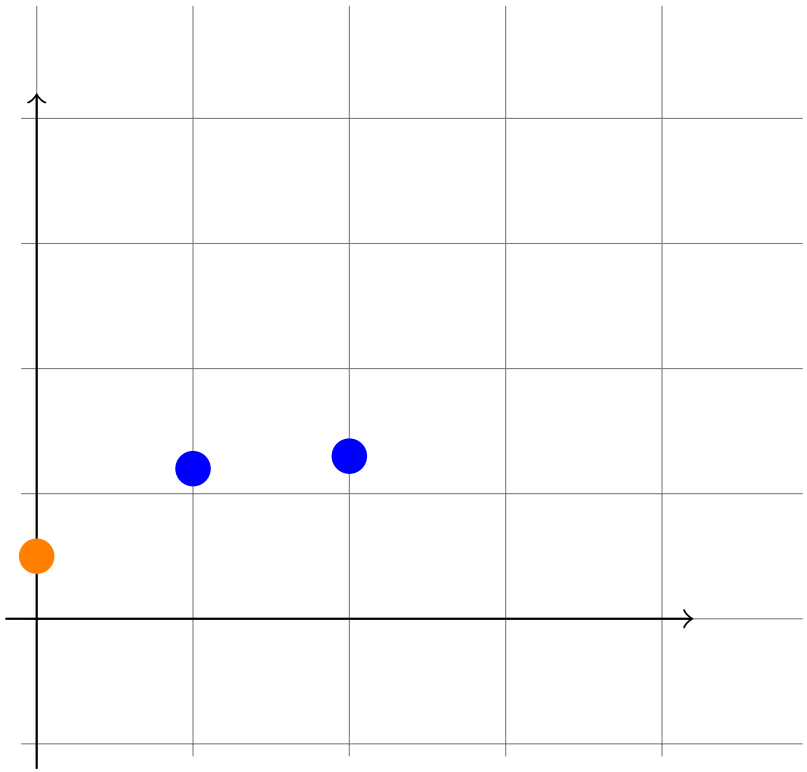
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



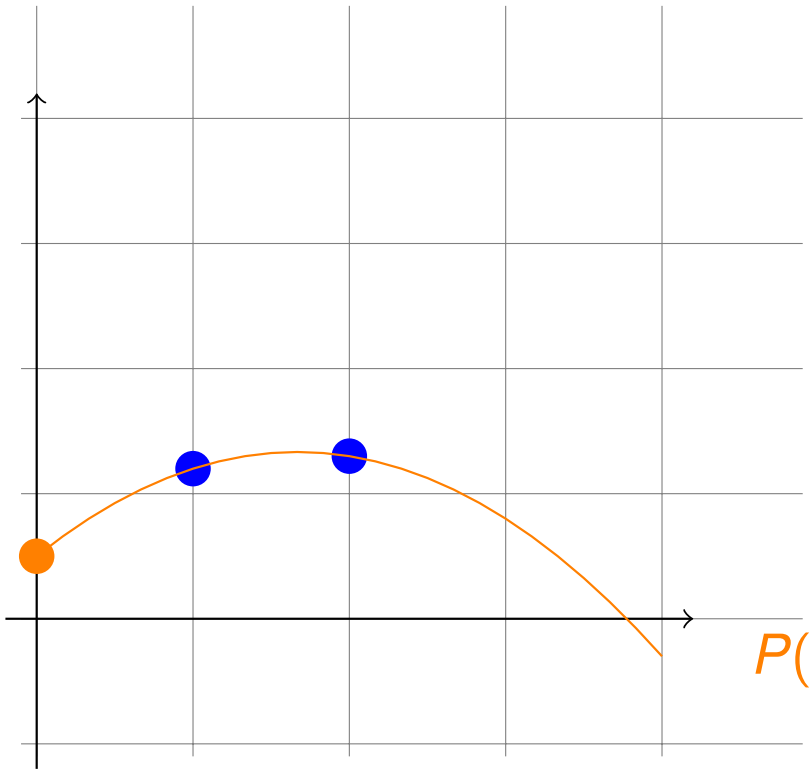
There is $P(x)$ contains blue points and *any* $(0, y)$!

2 points not enough.



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

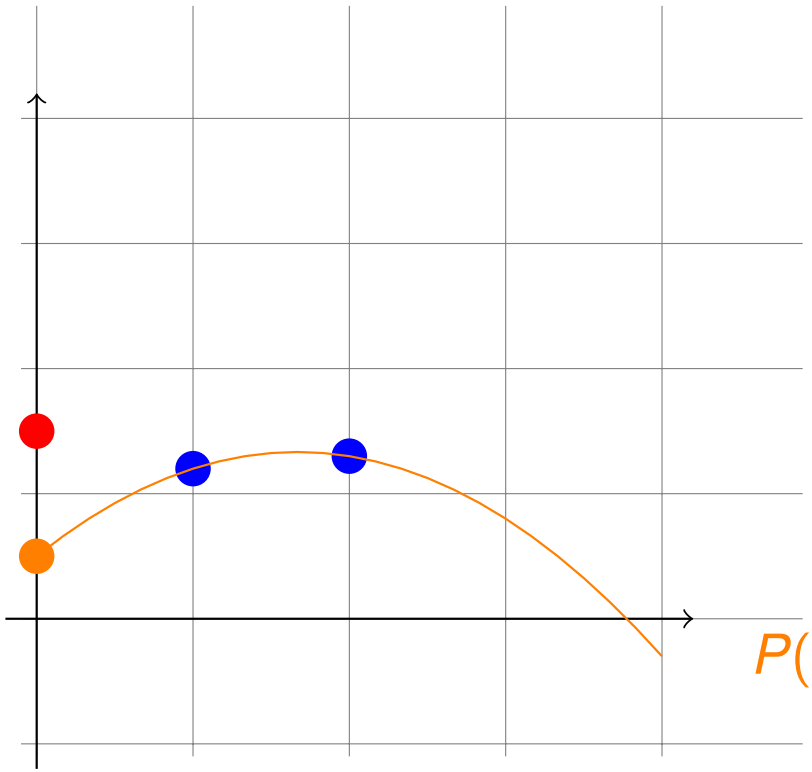
2 points not enough.



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

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

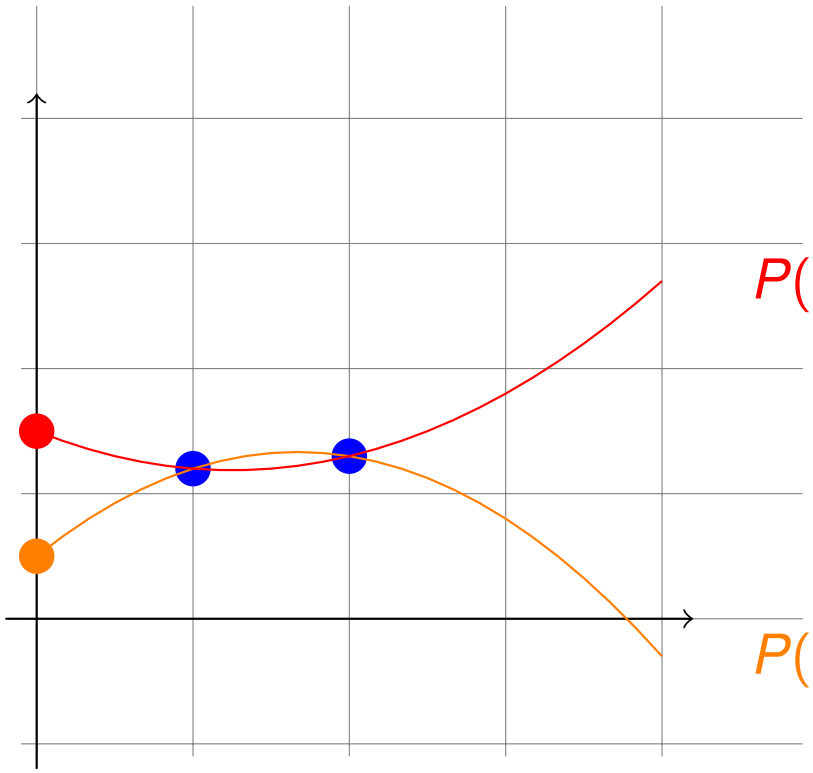
2 points not enough.



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

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

2 points not enough.

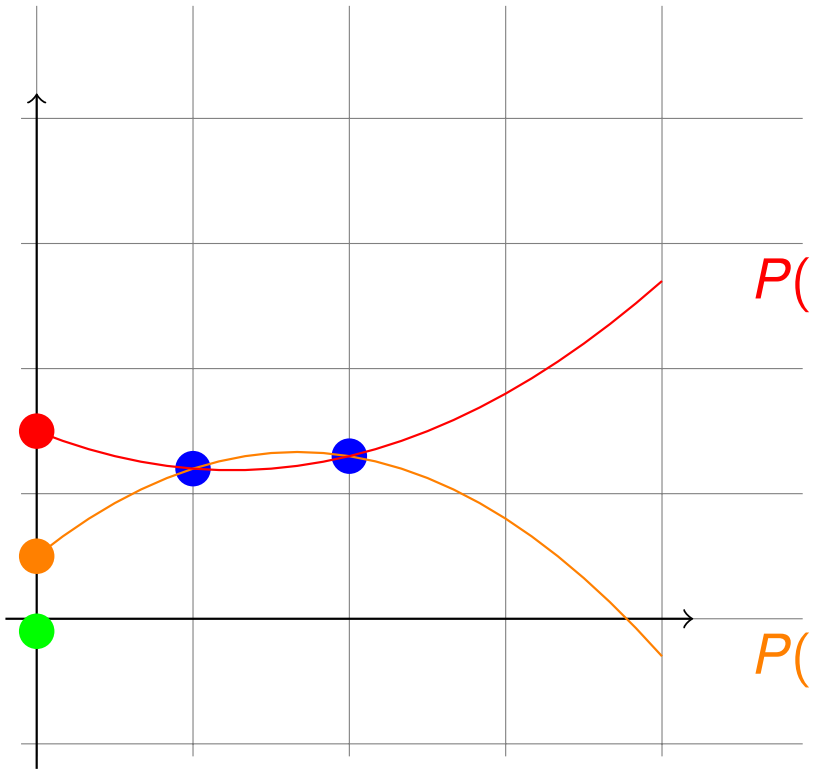


$P(x) = .2x^2 - .5x + 1.5$

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

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

2 points not enough.

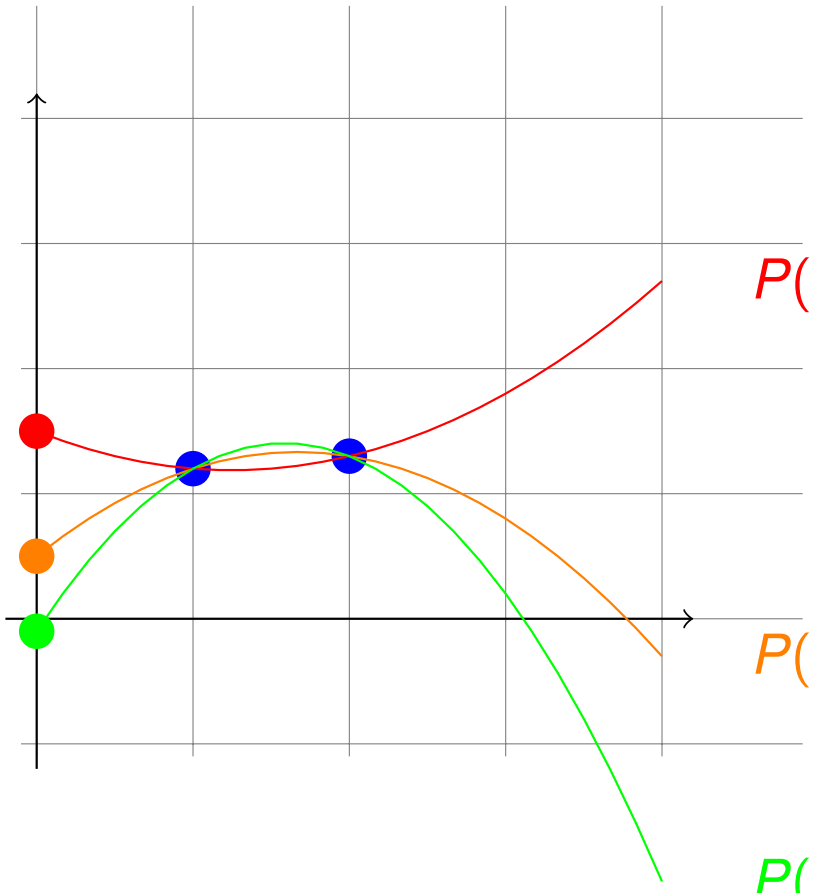


$P(x) = .2x^2 - .5x + 1.5$

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

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

2 points not enough.

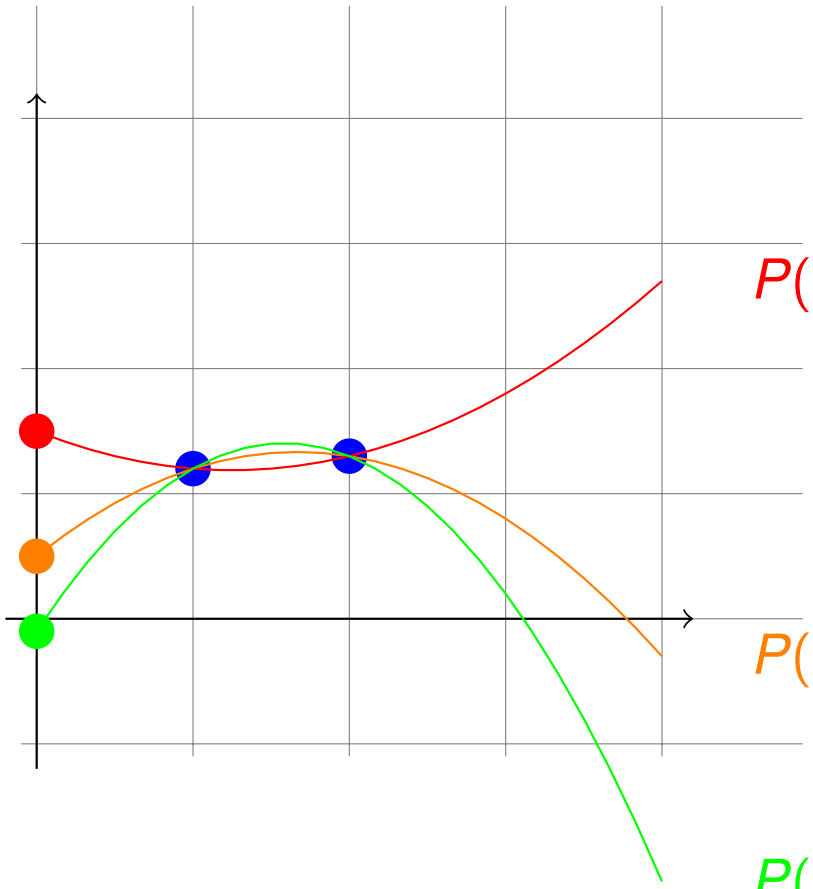


$P(x) = .2x^2 - .5x + 1.5$

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

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

2 points not enough.



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

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

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

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.

For $k = 2$?

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.

For $k = 2$? Two points determine a line!

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$,

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$, $m(2) + b$,

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$, $m(2) + b$, $\ldots$

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$, $m(2) + b$, $\ldots$
Any two determine line.

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$, $m(2) + b$, $\ldots$
Any two determine line. And b.

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$, $m(2) + b$, $\ldots$
Any two determine line. And b.
With only one point.

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.

For $k = 2$? Two points determine a line! $mx + b$.
Degree 1 polynomial.
Secret is b!!
Shares are $m(1) + b$, $m(2) + b$, $\ldots$
Any two determine line. And b.
With only one point. b can be anything!

We will work with polynomials with arithmetic modulo p.

Excursion.

Homework 4. Problem 2.

Excursion.

Homework 4. Problem 2.

$a = 1 \pmod 5$

Excursion.

Homework 4. Problem 2.

$a = 1 \pmod 5 \quad a = 0 \pmod 8$

Excursion.

Homework 4. Problem 2.

$a = 1 \pmod 5 \quad a = 0 \pmod 8$
$b = 0 \pmod 5$

Excursion.

Homework 4. Problem 2.

$$a = 1 \pmod 5 \quad a = 0 \pmod 8$$
$$b = 0 \pmod 5 \quad b = 1 \pmod 8$$

Excursion.

Homework 4. Problem 2.

$$a = 1 \pmod 5 \qquad a = 0 \pmod 8$$
$$b = 0 \pmod 5 \qquad b = 1 \pmod 8$$
$$c = 5 \pmod 5$$

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

What is c in terms of a and b?

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

What is c in terms of a and b?

$c =$

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

What is c in terms of a and b?

$c = 5a +$

Excursion.

Homework 4. Problem 2.

$$\begin{aligned} a &= 1 \pmod 5 & a &= 0 \pmod 8 \\ b &= 0 \pmod 5 & b &= 1 \pmod 8 \\ c &= 5 \pmod 5 & c &= 10 \pmod 8 \end{aligned}$$

What is c in terms of a and b?

$$c = 5a + 10b$$

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

What is c in terms of a and b?

$c = 5a + 10b$!!

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

What is c in terms of a and b?

$c = 5a + 10b$!!

Idea: a and b, 1 for one modulus and 0 for (all) others.

Excursion.

Homework 4. Problem 2.

$$\begin{array}{ll} a = 1 \pmod 5 & a = 0 \pmod 8 \\ b = 0 \pmod 5 & b = 1 \pmod 8 \\ c = 5 \pmod 5 & c = 10 \pmod 8 \end{array}$$

What is c in terms of a and b?

$c = 5a + 10b$!!

Idea: a and b, 1 for one modulus and 0 for (all) others.

See Chinese Remainder Theorem: many moduli.

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

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

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, combine Δ_i functions to contain 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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Delta Polynomials: Concept.

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

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

Given $d+1$ points, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
$(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$.

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

Does $y_1 \Delta_1(x) + y_2 \Delta_2(x)$ contain
(x_1, y_1)?

Delta Polynomials: Concept.

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

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

Given $d+1$ points, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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

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

Given $d+1$ points, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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

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

Given $d+1$ points, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

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

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

Given $d+1$ points, combine Δ_i functions to contain all points?
(x_1, y_1), ..., (x_{d+1}, y_{d+1}).

Will $y_1 \Delta_1(x)$ contain (x_1, y_1)? And is 0 for other x_i!

Will $y_2 \Delta_2(x)$ contain (x_2, y_2)? And is 0 for other x_i!

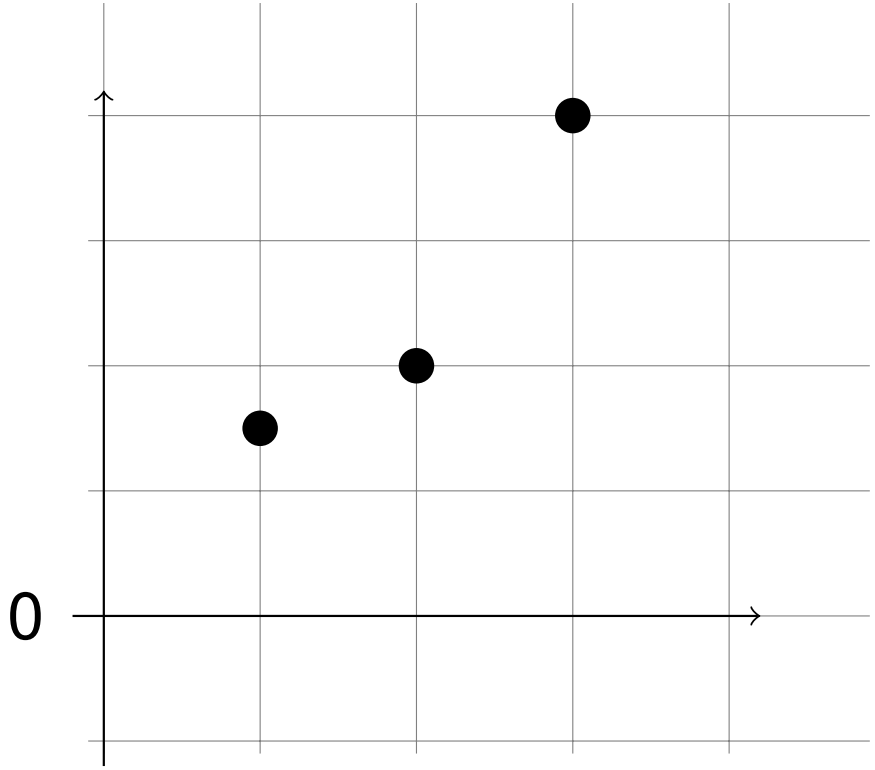
Does $y_1 \Delta_1(x) + y_2 \Delta_2(x)$ contain
(x_1, y_1)? and (x_2, y_2)?

See the idea? Function that contains all points?

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

Delta functions: in pictures.

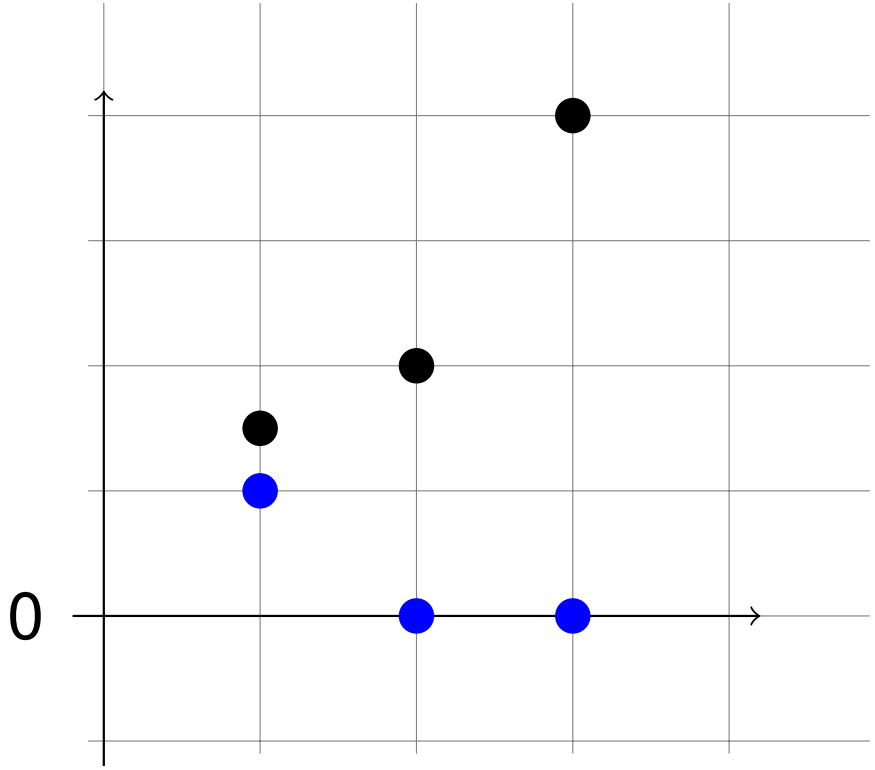
Points: $(1, 1.5)$, $(2, 2)$, $(3, 4)$.



Scale each Δ_i function and add to contain points.

Delta functions: in pictures.

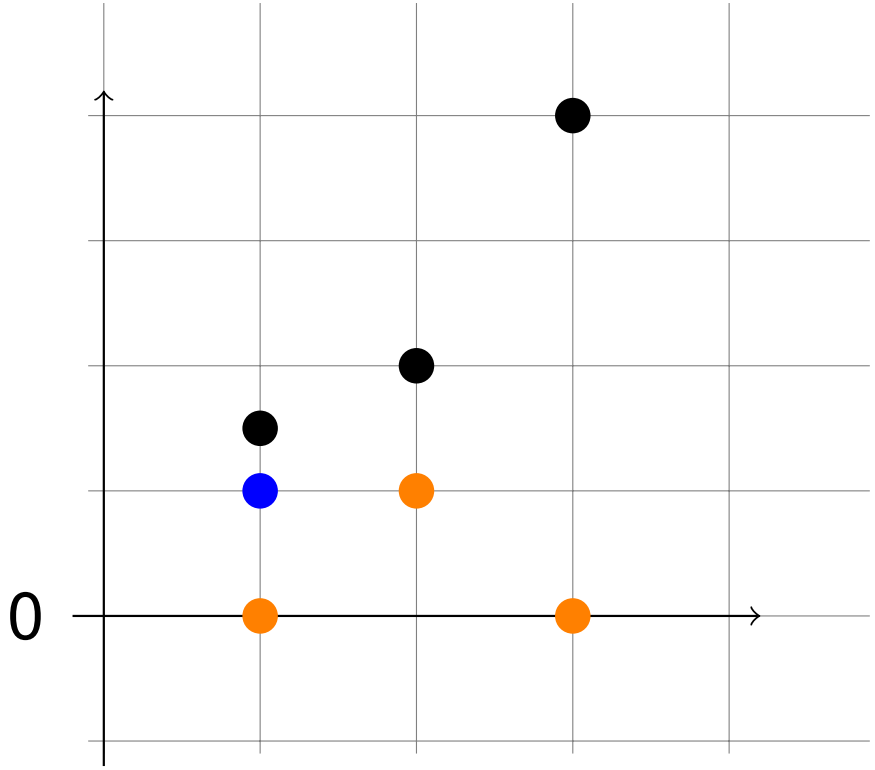
Points: $(1, 1.5)$, $(2, 2)$, $(3, 4)$.



Scale each Δ_i function and add to contain points.

Delta functions: in pictures.

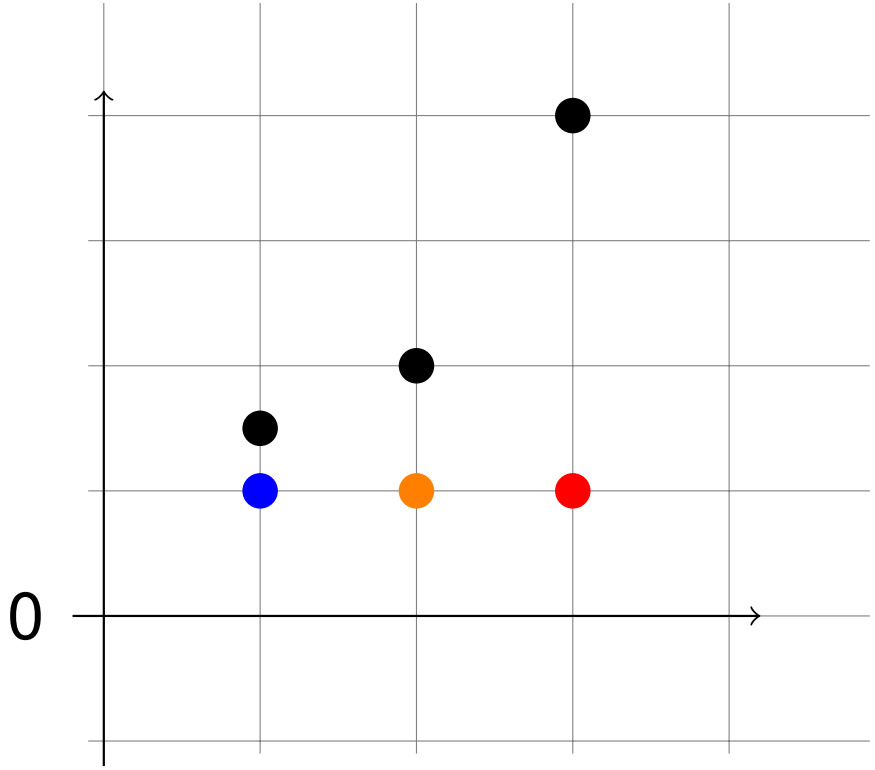
Points: $(1, 1.5)$, $(2, 2)$, $(3, 4)$.



Scale each Δ_i function and add to contain points.

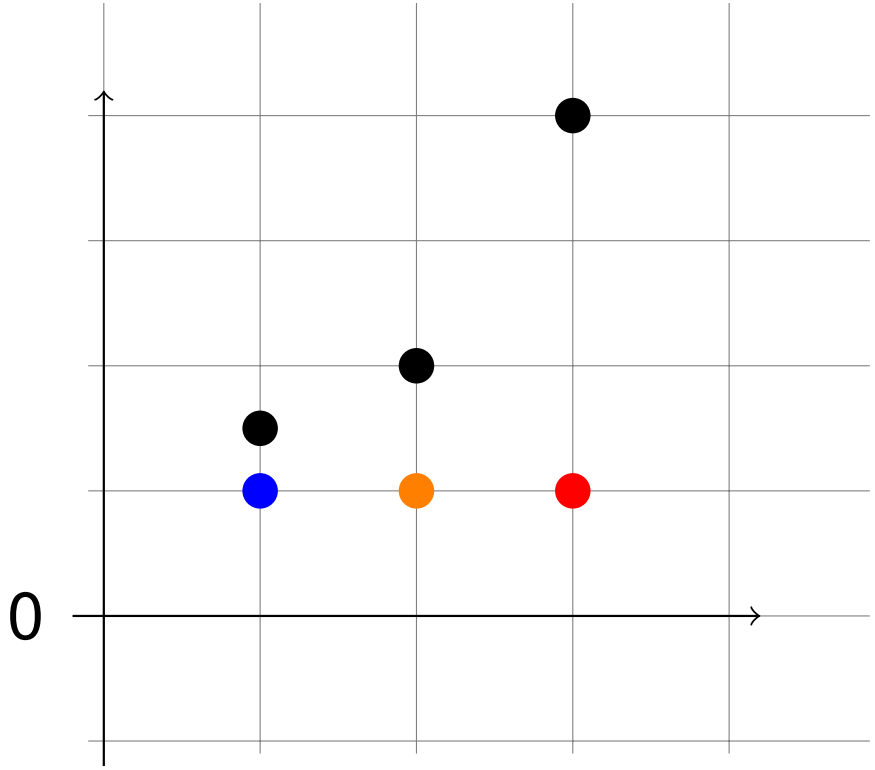
Delta functions: in pictures.

Points: $(1, 1.5)$, $(2, 2)$, $(3, 4)$.



Delta functions: in pictures.

Points: $(1, 1.5)$, $(2, 2)$, $(3, 4)$.



Scale each Δ_i function and add to contain points.

Delta functions and polynomials.

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

Delta functions and polynomials.

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

Work modulo 5.

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?

$\Delta_1(1) = 1$

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial?

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0$!

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well,

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

$\Delta_1(1) = 1$, $\Delta_1(3) = 0$

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

$\Delta_1(1) = 1$, $\Delta_1(3) = 0$
$\Delta_2(1) = 0$, $\Delta_2(3) = 1$

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

$\Delta_1(1) = 1$, $\Delta_1(3) = 0$
$\Delta_2(1) = 0$, $\Delta_2(3) = 1$

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

$\Delta_1(1) = 1$, $\Delta_1(3) = 0$
$\Delta_2(1) = 0$, $\Delta_2(3) = 1$

$P(x) = 3\Delta_1(x) + 4\Delta_2(x)$

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

$\Delta_1(1) = 1$, $\Delta_1(3) = 0$
$\Delta_2(1) = 0$, $\Delta_2(3) = 1$

$P(x) = 3\Delta_1(x) + 4\Delta_2(x)$

$P(x) = (x-3) + 2(x-1)$

Delta functions and polynomials.

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

Work modulo 5.

$\Delta_1(x)$?
$\Delta_1(1) = 1$ $\Delta_1(3) = 0$.

$\Delta_1(x)$ as polynomial? Focus on 0!

$f(x) = (x-3)$?

$f(3) = 0!$ $f(1) = -2 = 3 \pmod 5$!
Well, almost.
Divide by 3!

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

$\Delta_2(x) = 3(x-1) \pmod 5$.

$\Delta_1(1) = 1$, $\Delta_1(3) = 0$
$\Delta_2(1) = 0$, $\Delta_2(3) = 1$

$P(x) = 3\Delta_1(x) + 4\Delta_2(x)$

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

The Construction: Interpolation!

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

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

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

The 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.

The 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.

The 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!!

The 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.
$\Delta_1(x) = (x-2)(x-3)(3) \pmod 5$

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

The 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).

The 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).

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

The 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.

The 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?

The 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...

The 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 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!

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!

For secret sharing.

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

For secret sharing.

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

Proved existence.

For secret sharing.

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

Proved existence.

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

For secret sharing.

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

Proved existence.

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

Wednesday!