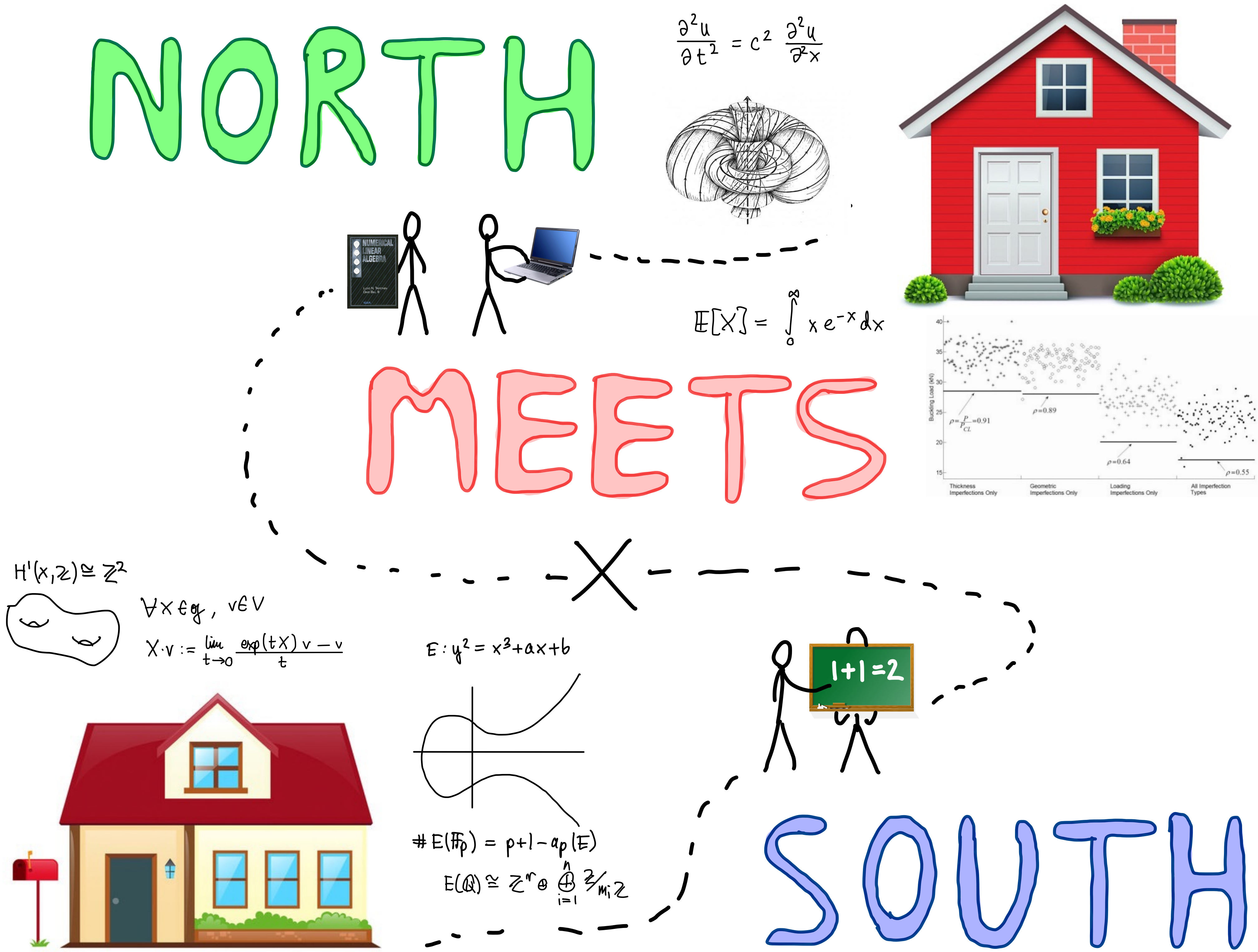
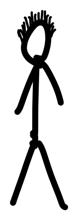

NORTH
MEETS
SOUTH
$\frac{\partial^2 u}{\partial t^2} = c^2 \frac{\partial^2 u}{\partial^2 x}$
NUMERICAL LINEAR ALGEBRA
$\mathbb{E}[X] = \int_0^\infty x e^{-x} dx$
Buckling Load (kN)
$\rho = \frac{P}{P_{CL}} = 0.91$
$\rho = 0.89$
$\rho = 0.64$
$\rho = 0.55$
Thickness Imperfections Only
Geometric Imperfections Only
Loading Imperfections Only
All Imperfection Types
$H^1(X,\mathbb{Z}) \cong \mathbb{Z}^2$
$\forall X \in \mathfrak{g},\ v \in V$
$X \cdot v := \lim_{t \to 0} \frac{\exp(tX)v - v}{t}$
$E : y^2 = x^3 + ax + b$
$\#E(\mathbb{F}_p) = p + 1 - a_p(E)$
$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$
$1+1=2$

BITCOIN

BITCOIN

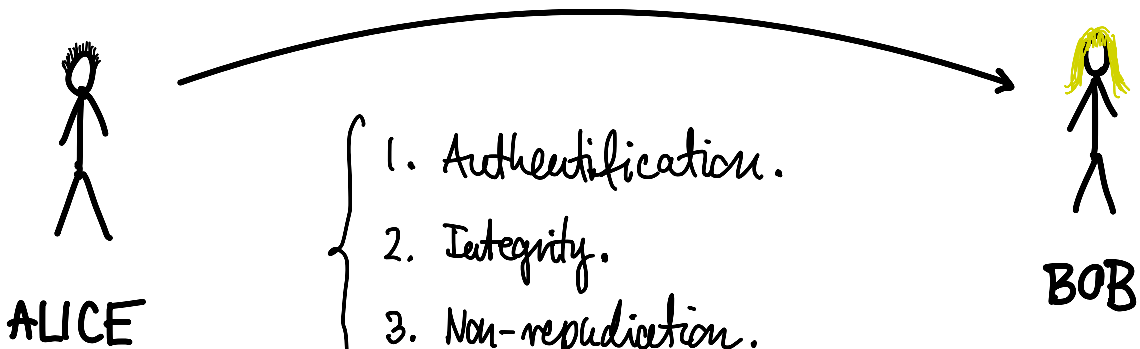
NEED: SECURE WAY TO SIGN A CONTRACT.



1. Authentification.
2. Integrity.
3. Non-repudiation.

BITCOIN

NEED: SECURE WAY TO SIGN A CONTRACT.



1. Authentification.
2. Integrity.
3. Non-repudiation.

BITCOIN

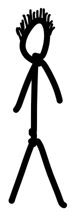
NEED: SECURE WAY TO SIGN A CONTRACT.

contract c

private key k

$\Downarrow$

signature (r, s)



ALICE

1. Authentification.
2. Integrity.
3. Non-repudiation.

BOB

contract c

signature (r, s)

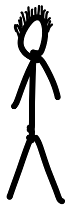
$\Downarrow$

Verify that (r, s) is a signature for c.

BITCOIN

NEED: SECURE WAY TO SIGN A CONTRACT.

contract c
private key k
signature (r, s)



ALICE

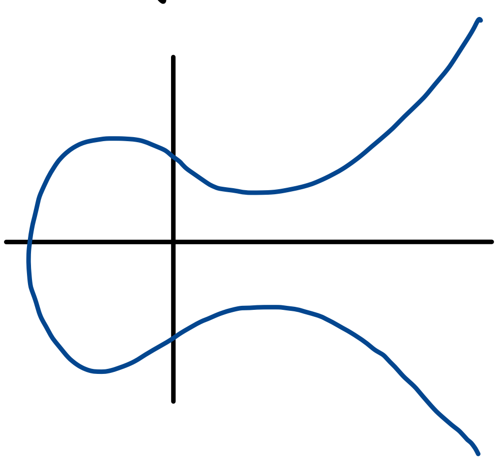
1. Authentification.
2. Integrity.
3. Non-repudiation.

BOB

contract c
signature (r, s)
Verify that (r, s) is a signature for c.

HOW? ELLIPTIC CURVES!

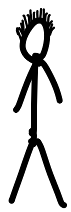
$$E : y^2 = x^3 + ax + b$$



BITCOIN

NEED: SECURE WAY TO SIGN A CONTRACT.

contract c
private key k
$\Downarrow$
signature (r, s)



ALICE

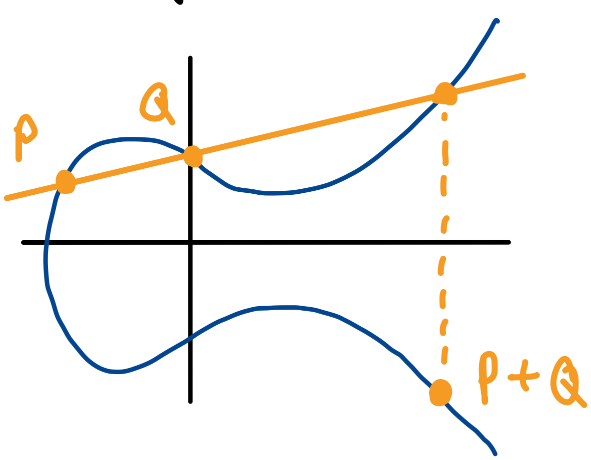
1. Authentification.
2. Integrity.
3. Non-repudiation.

BOB

contract c
signature (r,s)
$\Downarrow$
Verify that (r,s) is a signature for c.

HOW? ELLIPTIC CURVES!

$$E : y^2 = x^3 + ax + b$$

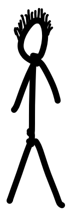


CAN ADD POINTS!

BITCOIN

NEED: SECURE WAY TO SIGN A CONTRACT.

contract c
private key k
⇓
signature (r, s)



ALICE

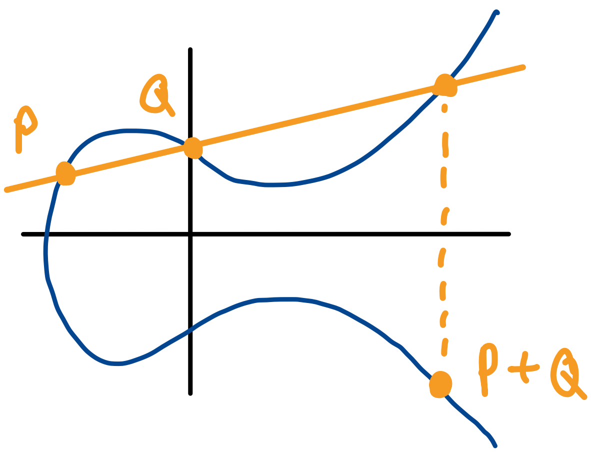
1. Authentification.
2. Integrity.
3. Non-repudiation.

BOB

contract c
signature (r, s)
⇓
Verify that (r, s) is a signature for c.

HOW? ELLIPTIC CURVES!

$$E: y^2 = x^3 + ax + b$$

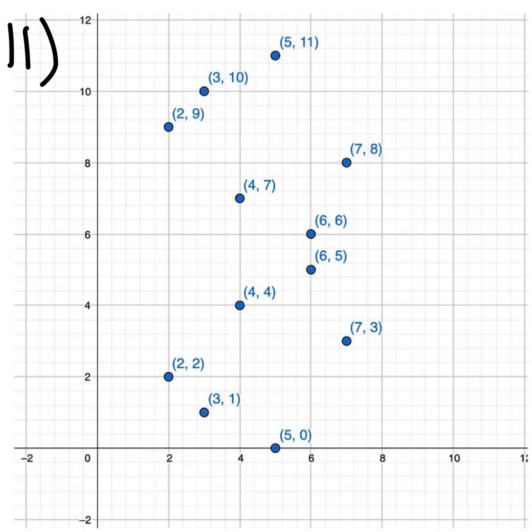


CAN ADD POINTS!

Instead, do this "modulo p":

$$E \bmod p: \quad y^2 \equiv x^3 + ax + b \mod p$$

$$(y^2 = x^3 + 7 \mod 11)$$
$$a = 0, b = 7$$
$$p = 11$$



BITCOIN

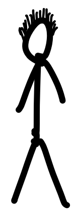
NEED: SECURE WAY TO SIGN A CONTRACT.

contract c

private key k

$\Downarrow$

signature (r, s)



ALICE

1. Authentification.
2. Integrity.
3. Non-repudiation.

BOB

contract c

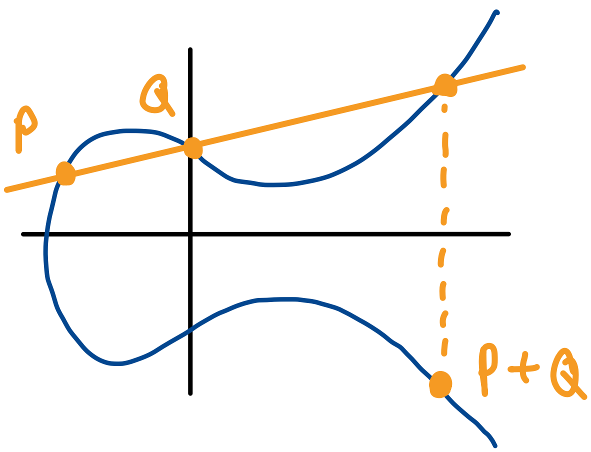
signature (r, s)

$\Downarrow$

Verify that (r, s) is a signature for c.

HOW? ELLIPTIC CURVES!

$$E : y^2 = x^3 + ax + b$$



CAN ADD POINTS!

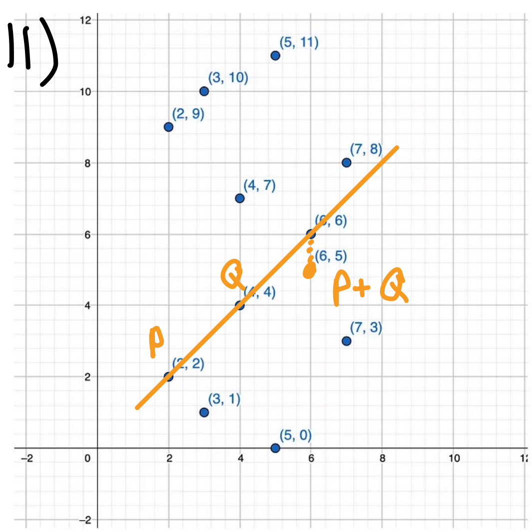
Instead, do this "modulo p":

$$E \bmod p: \quad y^2 \equiv x^3 + ax + b \mod p$$

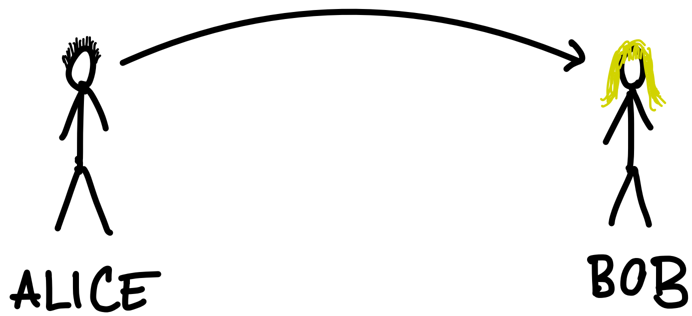
$(y^2 = x^3 + 7 \mod 11)$

$a = 0, b = 7$

$p = 11$



ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM



PUBLIC DATA:

- $a, b \rightsquigarrow E: y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to E mod p

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract: c
private key: k, d in $\{1, \ldots, N\}$

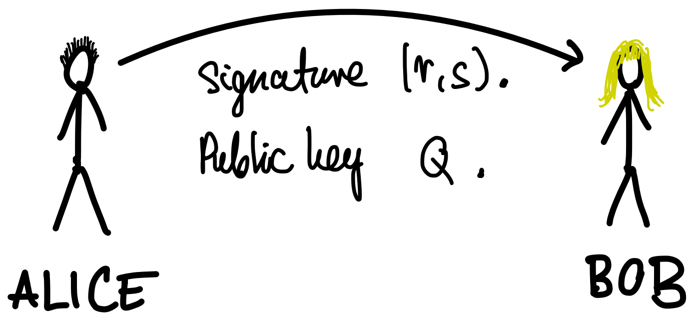
---

1. Compute $\underbrace{P + \cdots + P}_{k} = (x_1, y_1)$.

$r := x_1 \mod N$

$s := k^{-1}(c + rd) \mod N$

2. Compute: $Q = \underbrace{P + \cdots + P}_{d}$.



PUBLIC DATA:

- $a, b \rightsquigarrow E: y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \mod p$

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract: c
private key: k, d in $\{1, \dots, N\}$

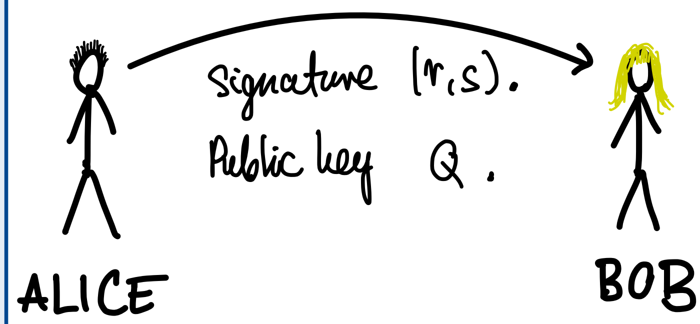
---

1. Compute $\underbrace{P + \dots + P}_{k} = (x_1, y_1)$.

$r := x_1 \bmod N$

$s := k^{-1}(c + rd) \bmod N$

2. Compute: $Q = \underbrace{P + \dots + P}_{d}$.



contract: c
signature: (r, s)
public key: Q

---

1. $u_1 := c \cdot s^{-1} \bmod N$
$u_2 := r \cdot s^{-1} \bmod N$

2. Compute:

$(x_1, y_1) = \underbrace{P + \dots + P}_{u_1} + \underbrace{Q + \dots + Q}_{u_2}$.

3. Signature valid if $r \equiv x_1 \bmod N$.

PUBLIC DATA:

- $a, b \rightsquigarrow E: y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \bmod p$

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract: c
private key: k, d in $\{1, \dots, N\}$

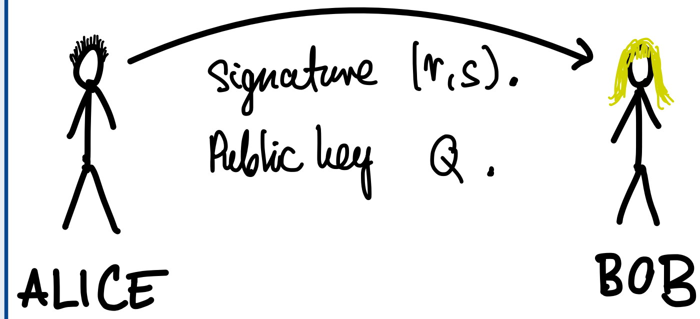
---

1. Compute $\underbrace{P + \dots + P}_{k} = (x_1, y_1)$.

$r := x_1 \mod N$

$s := k^{-1}(c + rd) \mod N$

2. Compute: $Q = \underbrace{P + \dots + P}_{d}$.



Proof it works.

$$
\begin{aligned}
u_1 P + u_2 Q &= u_1 P + u_2 d P \\
&= (u_1 + u_2 d) P \\
&= (c s^{-1} + r s^{-1} d) P \\
&= (c + rd) s^{-1} P \\
&= (c + rd)(c + rd)^{-1} k P \\
&= kP \checkmark
\end{aligned}
$$

contract: c
signature: (r, s)
public key: Q

---

1. $u_1 := c \cdot s^{-1} \mod N$
   $u_2 := r \cdot s^{-1} \mod N$

2. Compute:
   $(x_1, y_1) = \underbrace{P + \dots + P}_{u_1} + \underbrace{Q + \dots + Q}_{u_2}$.

3. Signature valid if $r \equiv x_1 \mod N$.

PUBLIC DATA:

- $a, b \rightsquigarrow E: y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \mod p$

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract : c
private key : k, d in $\{1, \dots, N\}$

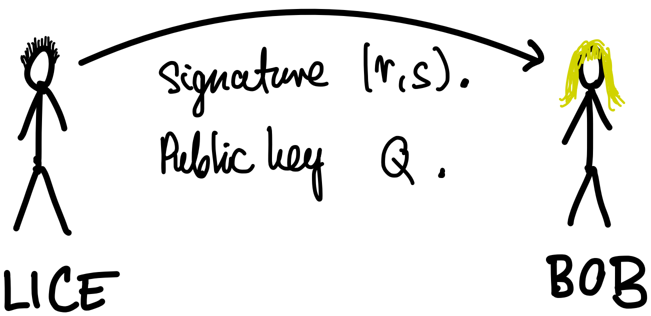
---

1. Compute $\underbrace{P + \dots + P}_{k} = (x_1, y_1)$.

   $r := x_1 \bmod N$

   $s := k^{-1}(c + rd) \bmod N$

2. Compute: $Q = \underbrace{P + \dots + P}_{d}$.



contract : c
signature : (r, s)
public key : Q

---

1. $u_1 := c \cdot s^{-1} \bmod N$
   $u_2 := r \cdot s^{-1} \bmod N$

2. Compute:
   $(x_1, y_1) = \underbrace{P + \dots + P}_{u_1} + \underbrace{Q + \dots + Q}_{u_2}$.

3. Signature valid if $r \equiv x_1 \bmod N$.

Proof it works.

$$
\begin{aligned}
u_1 P + u_2 Q &= u_1 P + u_2 d P \\
&= (u_1 + u_2 d) P \\
&= (c s^{-1} + r s^{-1} d) P \\
&= (c + rd) s^{-1} P \\
&= (c + rd)(c + rd)^{-1} k P \\
&= kP \checkmark
\end{aligned}
$$

PUBLIC DATA:

- $a, b \rightsquigarrow E : y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \bmod p$

BITCOIN'S CHOICES

- $a = 0, b = 7$

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract: c
private key: k, d in $\{1, \dots, N\}$

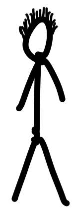
---

1. Compute $\underbrace{P + \cdots + P}_{k} = (x_1, y_1)$.

   $r := x_1 \mod N$

   $s := k^{-1}(c + rd) \mod N$

2. Compute: $Q = \underbrace{P + \cdots + P}_{d}$.



ALICE

$\xrightarrow{\text{Signature } (r,s).\ \text{Public key } Q.}$

BOB

contract: c
signature: (r, s)
public key: Q

---

1. $u_1 := c \cdot s^{-1} \mod N$
   $u_2 := r \cdot s^{-1} \mod N$

2. Compute:

   $(x_1, y_1) = \underbrace{P + \cdots + P}_{u_1} + \underbrace{Q + \cdots + Q}_{u_2}$.

3. Signature valid if $r \equiv x_1 \mod N$.

Proof it works.

$$
\begin{aligned}
u_1 P + u_2 Q &= u_1 P + u_2 d P \\
&= (u_1 + u_2 d) P \\
&= (c s^{-1} + r s^{-1} d) P \\
&= (c + rd) s^{-1} P \\
&= (c + rd)(c + rd)^{-1} k P \\
&= kP \checkmark
\end{aligned}
$$

PUBLIC DATA:

- $a, b \rightsquigarrow E: y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \mod p$

BITCOIN'S CHOICES

- $a = 0, b = 7$

The curve E: $y^2 = x^3+ax+b$ over F_p is defined by:

- a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
- b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract : c
private key : k, d in $\{1, \dots, N\}$

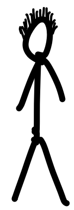
---

1. Compute $\underbrace{P + \dots + P}_{k} = (x_1, y_1)$.

$r := x_1 \mod N$

$s := k^{-1}(c + rd) \mod N$

2. Compute : $Q = \underbrace{P + \dots + P}_{d}$.



Signature (r, s).
Public key Q.

ALICE

BOB

contract : c
signature : (r, s)
public key : Q

---

1. $u_1 := c \cdot s^{-1} \mod N$
$u_2 := r \cdot s^{-1} \mod N$

2. Compute :
$(x_1, y_1) = \underbrace{P + \dots + P}_{u_1} + \underbrace{Q + \dots + Q}_{u_2}$.

3. Signature valid if $r \equiv x_1 \mod N$.

Proof it works.

$$
\begin{aligned}
u_1 P + u_2 Q &= u_1 P + u_2 d P \\
&= (u_1 + u_2 d) P \\
&= (c s^{-1} + r s^{-1} d) P \\
&= (c + rd) s^{-1} P \\
&= (c + rd)(c + rd)^{-1} k P \\
&= kP \ \checkmark
\end{aligned}
$$

PUBLIC DATA :

- $a, b \rightsquigarrow E : y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to E mod p

BITCOIN'S CHOICES

- $a = 0, b = 7$
- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
$= 11579209 \dots\dots$ (77 digits)

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

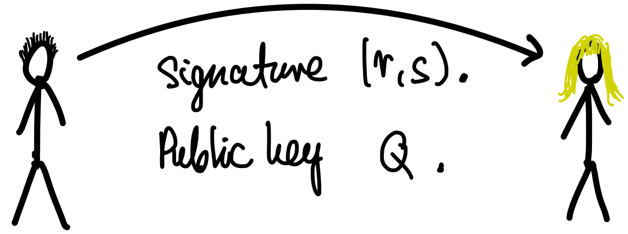
contract : c
private key : k, d in $\{1, \dots, N\}$

<u>1.</u> Compute $\underbrace{P + \cdots + P}_{k} = (x_1, y_1)$.

$r := x_1 \bmod N$

$s := k^{-1}(c + rd) \bmod N$

<u>2.</u> Compute: $Q = \underbrace{P + \cdots + P}_{d}$.



ALICE

BOB

contract : c
signature : (r, s)
public key : Q

<u>1.</u> $u_1 := c \cdot s^{-1} \bmod N$
$u_2 := r \cdot s^{-1} \bmod N$

<u>2.</u> Compute:

$(x_1, y_1) = \underbrace{P + \cdots + P}_{u_1} + \underbrace{Q + \cdots + Q}_{u_2}$.

<u>3.</u> Signature valid if $r \equiv x_1 \bmod N$.

Proof it works.

$$\begin{aligned} u_1 P + u_2 Q &= u_1 P + u_2 d P \\ &= (u_1 + u_2 d) P \\ &= (c s^{-1} + r s^{-1} d) P \\ &= (c + rd) s^{-1} P \\ &= (c + rd)(c + rd)^{-1} k P \\ &= kP \ \checkmark \end{aligned}$$

PUBLIC DATA:

- $a, b \rightsquigarrow E: y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \bmod p$

BITCOIN'S CHOICES

- $a = 0, b = 7$
- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
  $= 11579209 \dots\dots$ (77 digits)
- $P = \dots$

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

contract : c
private key : k, d in $\{1, \dots, N\}$

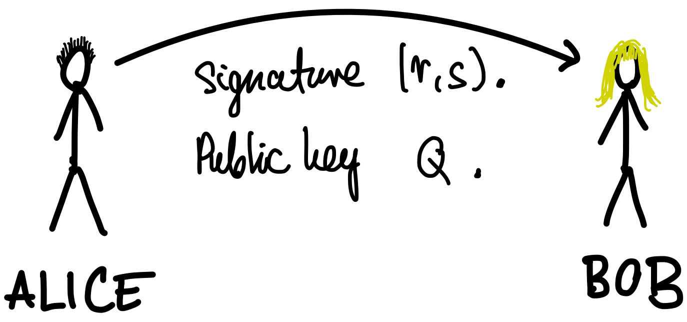
---

1. Compute $\underbrace{P + \dots + P}_{k} = (x_1, y_1)$.

$r := x_1 \bmod N$

$s := k^{-1}(c + rd) \bmod N$

2. Compute : $Q = \underbrace{P + \dots + P}_{d}$.



contract : c
signature : (r, s)
public key : Q

---

1. $u_1 := c \cdot s^{-1} \bmod N$
   $u_2 := r \cdot s^{-1} \bmod N$

2. Compute :
   $(x_1, y_1) = \underbrace{P + \dots + P}_{u_1} + \underbrace{Q + \dots + Q}_{u_2}$.

3. Signature valid if $r \equiv x_1 \bmod N$.

Proof it works.

$$\begin{aligned} u_1 P + u_2 Q &= u_1 P + u_2 d P \\ &= (u_1 + u_2 d) P \\ &= (c s^{-1} + r s^{-1} d) P \\ &= (c + rd) s^{-1} P \\ &= (c + rd)(c + rd)^{-1} k P \\ &= kP \ \checkmark \end{aligned}$$

PUBLIC DATA :

- $a, b \rightsquigarrow E : y^2 = x^3 + ax + b$
- p prime
- P point on E
- number $N = N_p(E)$ of solutions to $E \bmod p$

BITCOIN'S CHOICES

- $a = 0, b = 7$
- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
  $= 11579209 \dots\dots$ (77 digits)
- $P = \dots$
- $N = 11579209 \dots\dots$ (77 digits)

NOT HELPFUL ...

ELLIPTIC CURVES & MODULAR FORMS

MOTIVATION

Given E elliptic curve, what is $N_p(E) = \#$ of solutions to $y^2 \equiv x^3 + ax + b \mod p$?

Answer: $N_p(E) \approx p$ with error $a_p(E) := N_p(E) - p$, $|a_p(E)| \leq 2\sqrt{p}$.

$\Rightarrow$ Keep track of $a_p(E)$ instead of $N_p(E)$.

ELLIPTIC CURVES & MODULAR FORMS

MOTIVATION

Given E elliptic curve, what is $N_p(E) = \#$ of solutions to $y^2 \equiv x^3 + ax + b \mod p$?

<u>Answer:</u> $N_p(E) \approx p$ with error $a_p(E) := N_p(E) - p$, $|a_p(E)| \leq 2\sqrt{p}$.

$\Rightarrow$ Keep track of $a_p(E)$ instead of $N_p(E)$.

<u>Example:</u> $E : y^2 = x^3 + 7$

p	$N_p(E)$	$a_p(E)$
5	5	0
11	11	0
13	6	7
$\vdots$	$\vdots$	$\vdots$

ELLIPTIC CURVES & MODULAR FORMS

MOTIVATION

Given E elliptic curve, what is $N_p(E) = \#$ of solutions to $y^2 \equiv x^3 + ax + b \mod p$?

Answer: $N_p(E) \approx p$ with error $a_p(E) := N_p(E) - p$, $|a_p(E)| \leq 2\sqrt{p}$.

$\Rightarrow$ Keep track of $a_p(E)$ instead of $N_p(E)$.

Example: $E : y^2 = x^3 + 7$

p	$N_p(E)$	$a_p(E)$
5	5	0
11	11	0
13	6	7
$\vdots$	$\vdots$	$\vdots$
11579209... (77 digits)	11579209... (77 digits)	432420386565659656852420866390673177327 (38 digits)

ELLIPTIC CURVES & MODULAR FORMS

MOTIVATION

Given E elliptic curve, what is $N_p(E) = \#$ of solutions to $y^2 \equiv x^3 + ax + b \mod p$?

Answer: $N_p(E) \approx p$ with error $a_p(E) := N_p(E) - p$, $|a_p(E)| \leq 2\sqrt{p}$.

$\Rightarrow$ Keep track of $a_p(E)$ instead of $N_p(E)$.

Example: $E : y^2 = x^3 + 7$

p	$N_p(E)$	$a_p(E)$
5	5	0
11	11	0
13	6	7
$\vdots$	$\vdots$	$\vdots$
11579209 ... (77 digits)	11579209 ... (77 digits)	432420386565659656852420866390673177327 (38 digits)

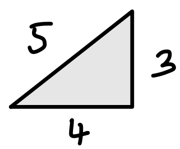
Modularity Theorem (Wiles, Taylor–Wiles, ...).

Given an elliptic curve E, there is a modular form $f(z) = \sum_{n=1}^{\infty} a_n \cdot (e^{2\pi i n z})$ $(z \in \mathbb{C}, \operatorname{Im} z > 0)$ such that $a_p = a_p(E)$ for all p.

MODULARITY THEOREM & FERMAT'S LAST THEOREM.

<u>Modularity Theorem</u> (Wiles, Taylor–Wiles, ...; 1995).

Given an elliptic curve E, there is a <u>modular form</u> $f(z) = \sum_{n=1}^{\infty} a_n \cdot (e^{2\pi i n z})$ $(z \in \mathbb{C}, \operatorname{Im} z > 0)$ such that $a_p = a_p(E)$ for all p.

There are triangles like 

$3^2 + 4^2 = 5^2$
$9 + 16 = 26$

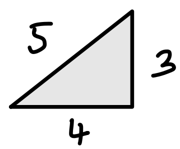
What about $a^n + b^n = c^n$ for $n \geq 3$? Fermat (1637): There are none.

MODULARITY THEOREM & FERMAT'S LAST THEOREM.

Modularity Theorem (Wiles, Taylor–Wiles, …; 1995).

Given an elliptic curve E, there is a modular form $f(z) = \sum_{n=1}^{\infty} a_n \cdot (e^{2\pi i n z})$ $(z \in \mathbb{C}, \operatorname{Im} z > 0)$ such that $a_p = a_p(E)$ for all p.

There are triangles like



$3^2 + 4^2 = 5^2$

$9 + 16 = 26$

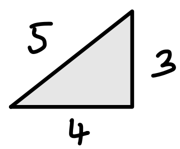
What about $a^n + b^n = c^n$ for $n \geq 3$? Fermat (1637): There are none.

Corollary. Fermat's Last Theorem: $\nexists$ a, b, c integers s.t. $a^n + b^n = c^n$ for $n \geq 3$.

MODULARITY THEOREM & FERMAT'S LAST THEOREM.

Modularity Theorem (Wiles, Taylor–Wiles, ...; 1995).

Given an elliptic curve E, there is a modular form $f(z) = \sum_{n=1}^{\infty} a_n \cdot (e^{2\pi i n z})$ $(z \in \mathbb{C}, \operatorname{Im} z > 0)$ such that $a_p = a_p(E)$ for all p.

There are triangles like  $3^2 + 4^2 = 5^2$
$9 + 16 = 26$

What about $a^n + b^n = c^n$ for $n \geq 3$? Fermat (1637): There are none.

Corollary. Fermat's Last Theorem: $\nexists$ a, b, c integers s.t. $a^n + b^n = c^n$ for $n \geq 3$.

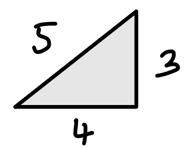
Pf sketch.

If they did exist, consider the elliptic curve: $y^2 = x(x - a^n)(x - b^n)$, Frey curve.

MODULARITY THEOREM & FERMAT'S LAST THEOREM.

Modularity Theorem (Wiles, Taylor–Wiles, ...; 1995).

Given an elliptic curve E, there is a modular form $f(z) = \sum_{n=1}^{\infty} a_n \cdot (e^{2\pi i n z})$ $(z \in \mathbb{C}, \operatorname{Im} z > 0)$ such that $a_p = a_p(E)$ for all p.

There are triangles like 

$3^2 + 4^2 = 5^2$
$9 + 16 = 26$

What about $a^n + b^n = c^n$ for $n \geq 3$? Fermat (1637): There are none.

Corollary. Fermat's Last Theorem: $\nexists$ a, b, c integers s.t. $a^n + b^n = c^n$ for $n \geq 3$.

Pf sketch.

If they did exist, consider the elliptic curve: $y^2 = x(x - a^n)(x - b^n)$, Frey curve.

Modularity $\Rightarrow$ $\exists$ modular form f associated to it.

Serre / Ribet $\Rightarrow$ such a modular form can't exist. $\square$

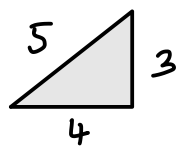
MODULARITY THEOREM & FERMAT'S LAST THEOREM.

Modularity Theorem (Wiles, Taylor–Wiles, …; 1995).

Given an elliptic curve E, there is a modular form $f(z) = \sum_{n=1}^{\infty} a_n \cdot (e^{2\pi i n z})$ $(z \in \mathbb{C}, \operatorname{Im} z > 0)$

such that $a_p = a_p(E)$ for all p.

There are triangles like



$3^2 + 4^2 = 5^2$

$9 + 16 = 26$

What about $a^n + b^n = c^n$ for $n \geq 3$? Fermat (1637): There are none.

Corollary. Fermat's Last Theorem: $\nexists$ a, b, c integers s.t. $a^n + b^n = c^n$ for $n \geq 3$.

Pf sketch.

If they did exist, consider the elliptic curve: $y^2 = x(x - a^n)(x - b^n)$, Frey curve.

Modularity $\Rightarrow$ $\exists$ modular form f associated to it.

Serre / Ribet $\Rightarrow$ such a modular form can't exist. $\square$

Rmk. James Newton (Oxford) & Ana Caraiani (Imperial) proved in 2023 that:

$E : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Q}(\sqrt{d})$ is modular!

BIRCH SWINNERTON-DYER CONJECTURE.

$E: \; y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$

$\rightsquigarrow E(\mathbb{Q})$ = solutions for $x, y \in \mathbb{Q}$ $\rightsquigarrow$ rank $r :=$ # of linearly indep. solutions.

BIRCH SWINNERTON-DYER CONJECTURE.

$E: \; y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$

$\rightsquigarrow E(\mathbb{Q})$ = solutions for $x, y \in \mathbb{Q}$ $\rightsquigarrow$ rank $r :=$ # of linearly indep. solutions.

Recall: $N_p(E) \approx p$ with some error.

BIRCH SWINNERTON-DYER CONJECTURE.

$E: \; y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$

$\rightsquigarrow E(\mathbb{Q})$ = solutions for $x, y \in \mathbb{Q}$ $\rightsquigarrow$ rank $r :=$ # of linearly indep. solutions.

Recall: $N_p(E) \approx p$ with some error.

(MILLENNIUM PRIZE PROBLEM, WORTH \$1,000,000.)

BSD Conjecture. $\displaystyle\prod_{p \leq X} \frac{N_p(E) + 1}{p} \approx C \cdot \log(x)^r$ as $x \longrightarrow \infty$

BIRCH SWINNERTON-DYER CONJECTURE.

$E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$

$\rightsquigarrow E(\mathbb{Q}) =$ solutions for $x, y \in \mathbb{Q}$ $\rightsquigarrow$ rank $r :=$ # of linearly indep. solutions.

Recall: $N_p(E) \approx p$ with some error.

(MILLENNIUM PRIZE PROBLEM, WORTH \$1,000,000.)

BSD Conjecture.

$$\underbrace{\prod_{p \leq X} \frac{N_p(E)+1}{p}}_{\text{only information mod } p \text{ for all } p} \approx C \cdot \underbrace{\log(x)^r}_{\text{information for } \mathbb{Q}} \quad \text{as } x \longrightarrow \infty$$