IT486 v3.0

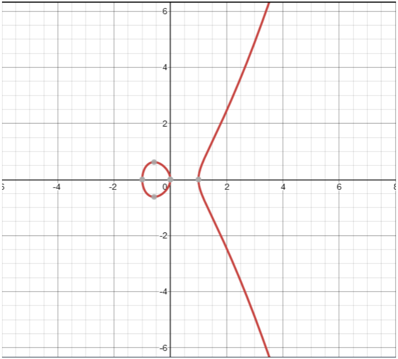
Elliptic Curves, ECDSA

Elliptic curves

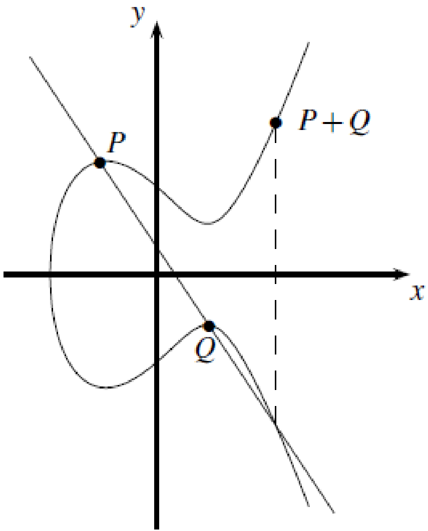
- An elliptic curve is the set

$$E = \{(x, y) : y^2 = x^3 + ax + b\}$$

- For example, when $a = -1$ and $b = 0$, we have $y^2 = x^3 - x$.

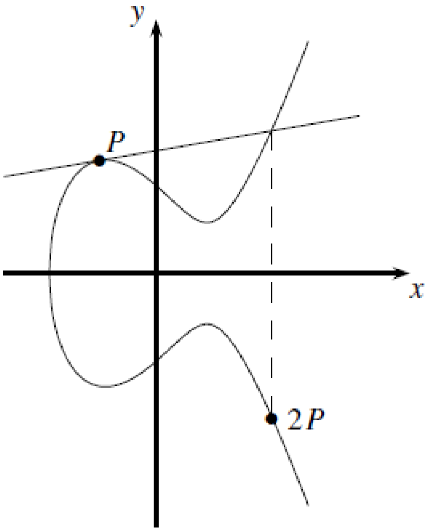


Point addition



- Draw a straight line through the two points P and Q
- It will intersect the elliptic curve in a third point
- Mirror that in the x-axis
- Note that this isn't just adding the coordinates

Point addition special case



- If $P = Q$, we can still add
- Here we use the tangent line to find a third point of intersection

Point addition special case

- What about if the line connecting P and Q is vertical?
- In this case we set $P + Q = \mathcal{O}$, where $\mathcal{O}$ is a special point called point at infinity

Point addition special case

- What about if the line connecting P and Q is vertical?
- In this case we set $P + Q = \mathcal{O}$, where $\mathcal{O}$ is a special point called point at infinity
- Assume this point lies on every vertical line
- For all points on the curve, $P + \mathcal{O} = P$ (the point at infinity acts like zero for elliptic curve addition)

Elliptic curve group

- Point addition gets us a group!
- Closure: For all P, Q in $E \Rightarrow P + Q$ is also in E.

Elliptic curve group

- Point addition gets us a group!
- Closure: For all P, Q in $E \Rightarrow P + Q$ is also in E.

  Clear from the definition of addition operation

Elliptic curve group

- Point addition gets us a group!
- Closure: For all P, Q in $E \Rightarrow P + Q$ is also in E.

  Clear from the definition of addition operation

- Identity: There is an element I in E such that for all P in E:

$$P + I = I + P = P$$

Elliptic curve group

- Point addition gets us a group!
- Closure: For all P, Q in $E \Rightarrow P + Q$ is also in E.

Clear from the definition of addition operation

- Identity: There is an element I in E such that for all P in E:

$$P + I = I + P = P$$

The identity element is $I = \mathcal{O}$

Elliptic curve group

- Point addition gets us a group!
- Inverse: For all P in E there is an element P' in E such that

$$P + P' = \mathcal{O}$$

Elliptic curve group

- Point addition gets us a group!
- Inverse: For all P in E there is an element P' in E such that

$$P + P' = \mathcal{O}$$

> Suppose $P = (x, y)$, then $P' = (x, -y)$ is also in E. Moreover, $P + P' = \mathcal{O}$.

- We write $P' = -P$

Elliptic curve group

- Point addition gets us a group!

Elliptic curve group

- Point addition gets us a group!
- Associativity: For all P, Q, R in E,

$$(P + Q) + R = P + (Q + R)$$

Elliptic curve group

- Point addition gets us a group!
- Associativity: For all P, Q, R in E,

$$(P+Q)+R = P+(Q+R)$$

We can show this using the formulas for adding points

Elliptic curve group

- Point addition gets us a group!
- Associativity: For all P, Q, R in E,

$$(P + Q) + R = P + (Q + R)$$

> We can show this using the formulas for adding points

- Commutativity: For all P, Q in $E \Rightarrow P + Q = Q + P$

Elliptic curve group

- Point addition gets us a group!
- Associativity: For all P, Q, R in E,

$$(P+Q)+R = P+(Q+R)$$

We can show this using the formulas for adding points

- Commutativity: For all P, Q in $E \Rightarrow P+Q = Q+P$

Clear from the definition of the addition operation

Formulas for adding points

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $x_1 \neq x_2$

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

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$$

$$s = (y_2 - y_1)/(x_2 - x_1)$$

$$\begin{aligned} x_3 &= s^2 - x_1 - x_2 \\ y_3 &= s(x_1 - x_3) - y_1 \end{aligned}$$

Formulas for adding points

Let $P = (x_1, y_1)$, $Q = (x_1, y_1)$

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

$$(x_3, y_3) = (x_1, y_1) + (x_1, y_1)$$

$$s = (3x_1^2 + a)/(2y_1)$$

$$\begin{aligned} x_3 &= s^2 - 2x_1 \\ y_3 &= s(x_1 - x_3) - y_1 \end{aligned}$$

What is a Finite Field?

- Has only finitely many elements
- Closed under $+$, $-$, $\times$, $/$, except division by 0
- Every nonzero element has a multiplicative inverse
- Ex: Prime Field of Order 19 (Denoted F_{19})

  $F_{19} = \{0, 1, 2, \ldots, 18\}$

Finite Field Arithmetic

Same as modulo P arithmetic (F_{19})

$8 + 14 = 22 \ \% \ 19 = 3$

$4 - 12 = -8 \ \% \ 19 = 11$

$17 - 6 = 11 \ \% \ 19 = 11$

$2 * 4 = 8 \ \% \ 19 = 8$

$11^3 = 1331 \ \% \ 19 = 1$

Defining Elliptic Curve over Finite Field

- Let $E : y^2 = x^3 + ax + b$ with $a, b \in F_p$
- Look at the points on E with coordinates in F_p (Denoted by $E(F_p)$)

Defining Elliptic Curve over Finite Field

- Let $E : y^2 = x^3 + ax + b$ with $a, b \in F_p$
- Look at the points on E with coordinates in F_p (Denoted by $E(F_p)$)
- Example:

$$E(F_5) = \{(x, y) : x, y \in F_5 \text{ satisfying } y^2 = x^3 + 4x + 4 \bmod 5\}$$

Defining Elliptic Curve over Finite Field

- Let $E : y^2 = x^3 + ax + b$ with $a, b \in F_p$
- Look at the points on E with coordinates in F_p (Denoted by $E(F_p)$)
- Example:

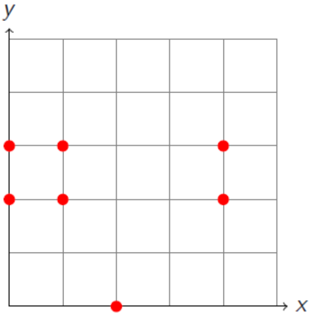
$$E(F_5) = \{(x, y) : x, y \in F_5 \text{ satisfying } y^2 = x^3 + 4x + 4 \bmod 5\}$$

- The points of $E(F_5)$ are:
  - $x = 0$ gives $y^2 = 4$ so that $y = 2$ or $y = 3$
  - $x = 1$ gives $y^2 = 9 = 4$ so that $y = 2$ or $y = 3$
  - $x = 2$ gives $y^2 = 20 = 0$ so that $y = 0$
  - $x = 3$ gives $y^2 = 43 = 3$, no square root
  - $x = 4$ gives $y^2 = 84 = 4$ so that $y = 2$ or $y = 3$

Defining Elliptic Curve over Finite Field

- $E(F_5)$ consists of 8 points:

$$E(F_5) = \{(0,2),(0,3),(1,2),(1,3),(2,0),(4,2),(4,3)\} \cup \{\mathcal{O}\}$$



Subgroups of order n

- Start with an elliptic curve over a finite field
- Pick a point G (generator point)

Subgroups of order n

- Start with an elliptic curve over a finite field
- Pick a point G (generator point)
- Repeatedly add G to itself: $G + G = 2G$, $G + G + G = 3G$, $\ldots$, $nG = \mathcal{O}$ (point at infinity)
- The smallest such n is called the order of G

Subgroups of order n

- Start with an elliptic curve over a finite field
- Pick a point G (generator point)
- Repeatedly add G to itself: $G + G = 2G$, $G + G + G = 3G$, $\dots$, $nG = \mathcal{O}$ (point at infinity)
- The smallest such n is called the order of G
- The set $\{\mathcal{O}, G, 2G, \dots, (n-1)G\}$ is subgroup of order n

Scalar multiplication

- Imagine a really large group $n \sim 2^{256}$
- $P = sG$ where s is really, really large

Scalar multiplication

- Imagine a really large group $n \sim 2^{256}$
- $P = sG$ where s is really, really large
- Finding P when we know s is easy

Scalar multiplication

- Imagine a really large group $n \sim 2^{256}$
- $P = sG$ where s is really, really large
- Finding P when we know s is easy
- Finding s when we know P is not
- We call s the discrete logarithm of P with respect to G; we write $s = \log_G P$

Scalar multiplication

- Imagine a really large group $n \sim 2^{256}$
- $P = sG$ where s is really, really large
- Finding P when we know s is easy
- Finding s when we know P is not
- We call s the discrete logarithm of P with respect to G; we write $s = \log_G P$
- Convention: lower-case letters for secrets, upper-case letters for points

The Bitcoin Elliptic Curve: secp256k1

- Equation $y^2 = x^3 + 7$ ($a = 0$, $b = 7$)
- Prime (p) $= 2^{256} - 2^{32} - 977$

The Bitcoin Elliptic Curve: secp256k1

- Equation $y^2 = x^3 + 7$ ($a = 0$, $b = 7$)
- Prime (p) $= 2^{256} - 2^{32} - 977$
- Generator point (G) $=$

  ```
  (0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798,
   0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8)
  ```

- Order (n) $=$

  ```
  0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
  ```

The Bitcoin Elliptic Curve: secp256k1

- Equation $y^2 = x^3 + 7$ $(a = 0,\ b = 7)$
- Prime $(p) = 2^{256} - 2^{32} - 977$
- Generator point $(G) =$

```
(0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798,
 0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8)
```

- Order $(n) =$

```
0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
```

- SEC = Standards for Efficient Cryptography
- 256 = number of bits in the prime order of the field

Public Key Cryptography

- Private key is the scalar (Denoted w/lower-case letter "s")
- Public key is the resulting point sG (Denoted w/upper-case letter "P")

Public Key Cryptography

- Private key is the scalar (Denoted w/lower-case letter "s")
- Public key is the resulting point sG (Denoted w/upper-case letter "P")
- Public key is a point (x, y) and thus has 2 numbers

SEC Format

- Public key (point on curve) serialized
- Uncompressed (65 bytes)

```
047211a824f55b505228e4c3d5194c1fcfaa15a456abdf37f9b9d97a4040afc073dee6c8906498
4f03385237d92167c13e236446b417ab79a0fcae412ae3316b77

        - 04 - Marker
        - x coordinate - 32 bytes
        - y coordinate - 32 bytes
```

SEC Format

- Public key (point on curve) serialized
- Uncompressed (65 bytes)

```
047211a824f55b505228e4c3d5194c1fcfaa15a456abdf37f9b9d97a4040afc073dee6c8906498
4f03385237d92167c13e236446b417ab79a0fcae412ae3316b77

- 04 - Marker
- x coordinate - 32 bytes
- y coordinate - 32 bytes
```

- Compressed

```
0349fc4e631e3624a545de3f89f5d8684c7b8138bd94bdd531d2e213bf016b278a

- 02 if y is even, 03 if odd - Marker
- x coordinate - 32 bytes
```

Take home problem

Consider the elliptic curve E defined over F_5 and point P given by:

$$E : y^2 = x^3 + 2x - 1 \pmod 5; \;\; P = (0, 2).$$

1. Determine the tangent l through P to this curve
2. Find the point Q different from P that lies on l and E
3. Determine $2P$ on E