타 원 곡 선 암 호

Elliptic Curves Cryptography (ECC)

https://youtu.be/_GOmrsCbNss

Elliptic Curves Cryptography

- ECC, ECDH, ECDSA?

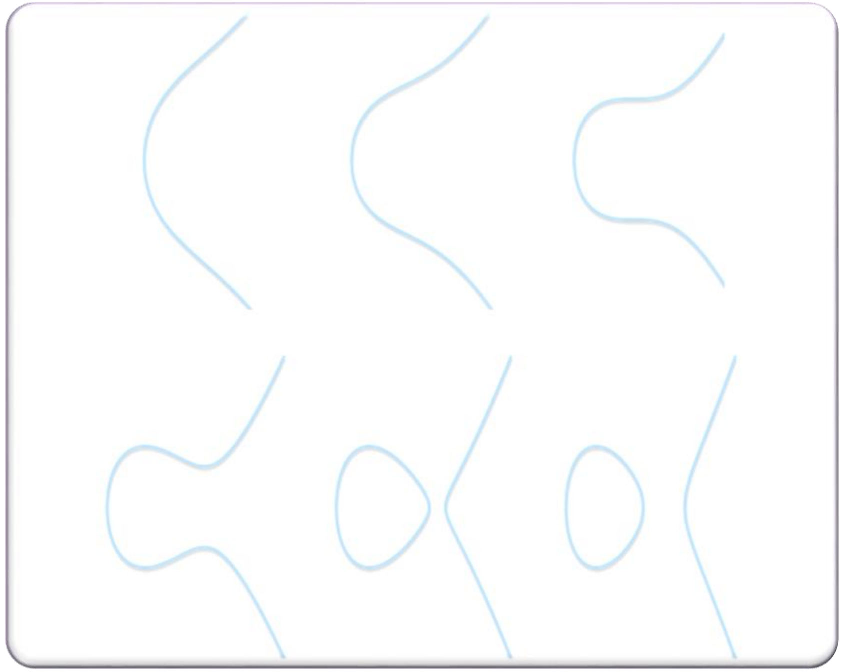
Name	Example
TLS (Transport Layer Security)	HTTPs
SSH (Security SHell)	Remote control
PGP (Pretty Good Privacy)	E-mail
Cryptocurrencies	Bitcoin

→ Internet Security

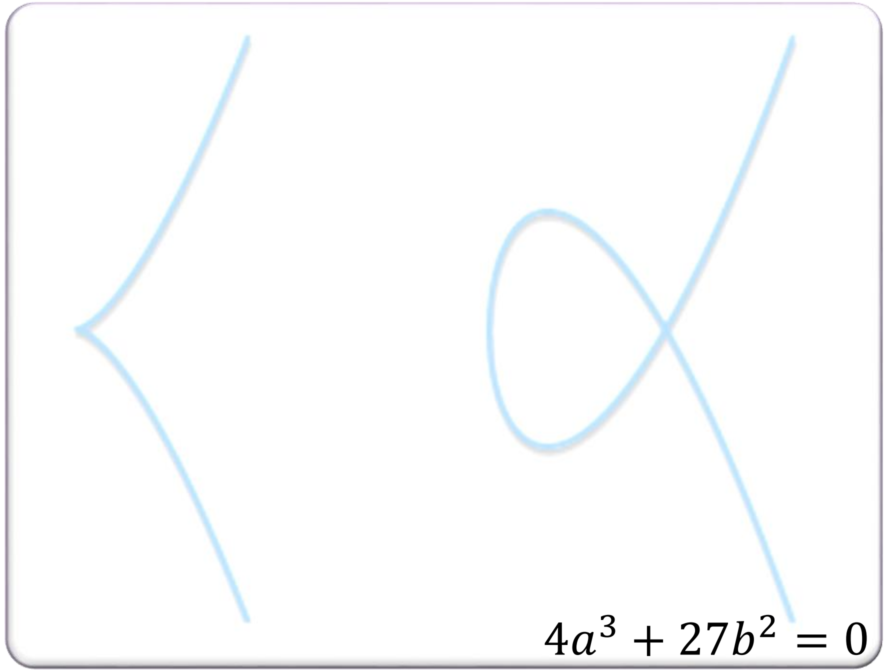
Elliptic Curves

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

Normal Form



Singularity Form



$$\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$

Groups

- $Addition\ (+)$
  - Closure
  - Associativity
  - Identity element
  - Inverse element

  - **Commutativity → Abelian group**

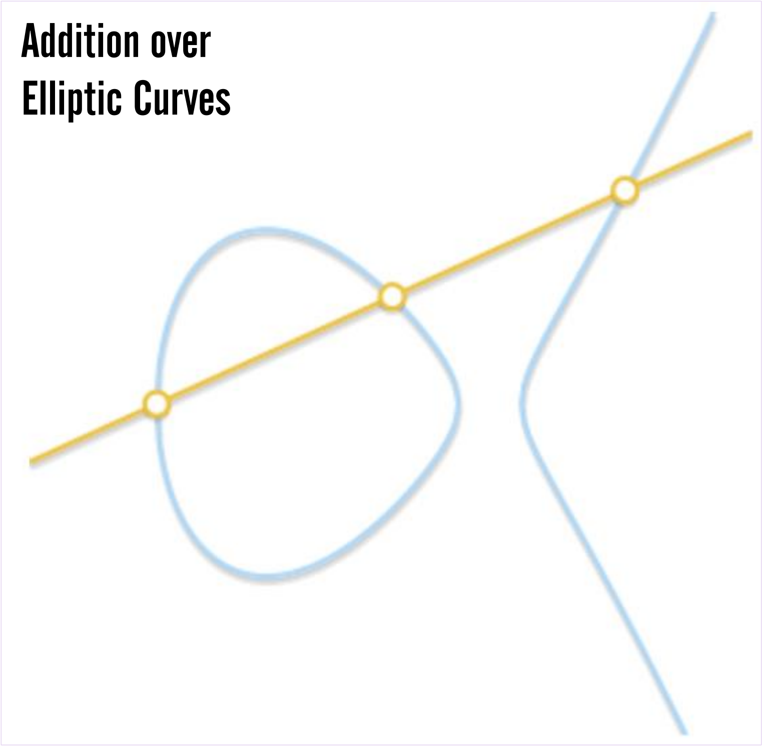
Example : $\mathbb{Z}\ (\ a\ group\ ),\ \mathbb{N}(\ not\ a\ group\ )$

$\mathbb{Z}$ ↓ Have Inverse Element

$\mathbb{N}$ ↓ Doesn't Have Inverse Element

Elliptic Curves over Group

- Elements
  - Points of an curve
- Identity element
  - Point at infinity or Ideal point → 0
- Inverse element
  - Point symmetric about x-axis;
- Addition
  - Given **aligned** three points P, Q, R → $P + Q + R = 0$
    (associative, commutative)



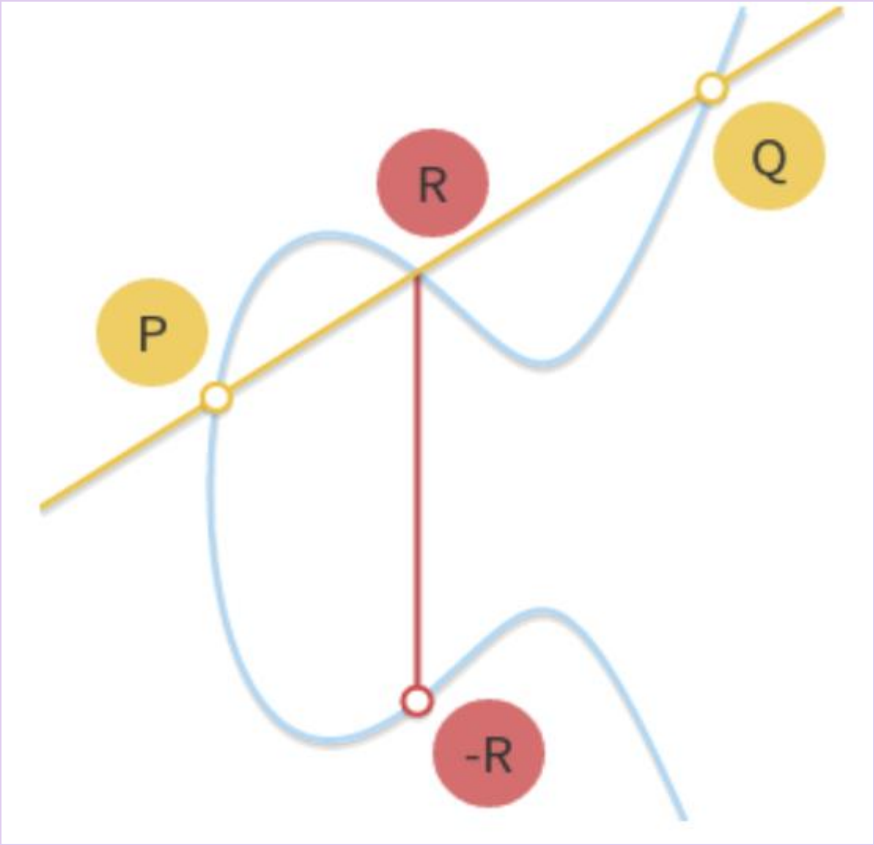
Geometric Addition

$$P + Q + R = 0, P + Q = -R$$

$P = 0\ or\ Q = 0$
→Identity element

$P = -Q$
→ Inverse element

$P = Q\ or\ P \neq Q\ but\ no\ R$
→ Tangency



Algebraic Addition

- $P + 0 = 0 + P = P, P + (-P) = 0$
- Points P, Q, R

$$m = \frac{y_P - y_Q}{x_P - x_Q}$$

Tangency

$$m = \frac{3x_P^2 + a}{2y_P}$$

$$\begin{aligned} x_R &= m^2 - x_P - x_Q \\ y_R &= y_P + m(x_R - x_P) \end{aligned}$$

$$y_R = y_Q + m(x_R - x_Q)$$

Formula

Roots of the Cubic Equation

$$ax^3 + bx^2 + cx + d = 0 \ (a \neq 0)$$

$$x_1 = -\frac{b}{3a} - \frac{1}{3a}A - \frac{1}{3a}B$$
$$x_2 = -\frac{b}{3a} + \frac{1 + i\sqrt{3}}{6a}A + \frac{1 - i\sqrt{3}}{6a}B$$
$$x_3 = -\frac{b}{3a} + \frac{1 - i\sqrt{3}}{6a}A + \frac{1 + i\sqrt{3}}{6a}B$$

$$y^2 = x^3 + ax + b$$
$$y = y_P + m(x - x_P)$$

$$x^3 + ax + b$$
$$= \{y_P + m(x - x_P)\}^2$$

$$x^3 - m^2x^2 \cdots + b = 0$$
$$x_P + x_Q + x_R = m^2$$
$$\therefore \boldsymbol{x_R = m^2 - x_P - x_Q}$$

Formula

$$m = \frac{3x_P^2 + a}{2y_P}$$

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

→

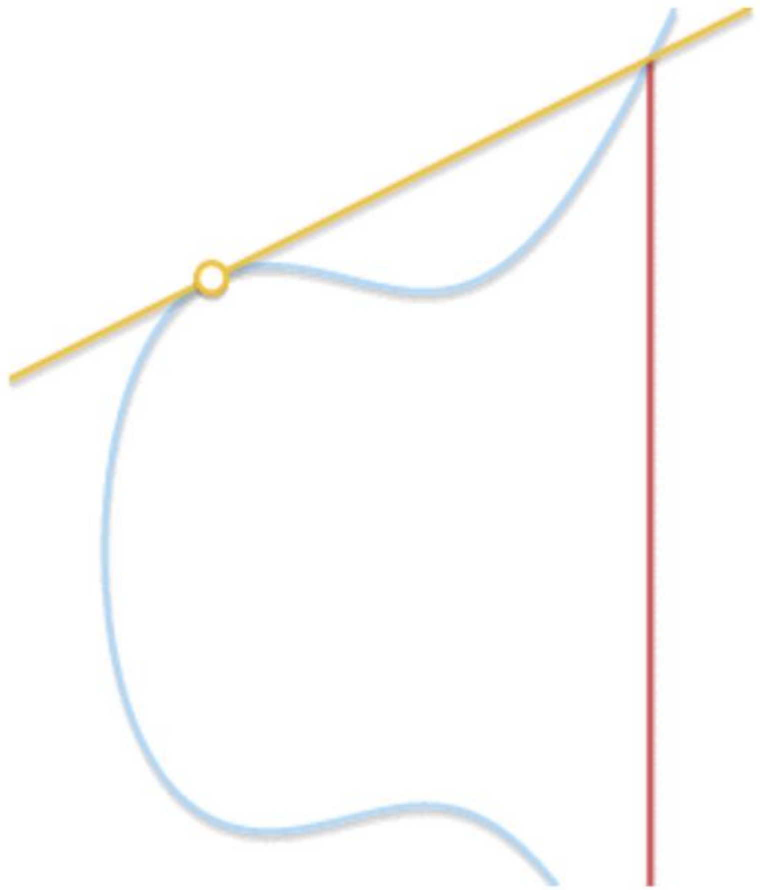
Scalar Multiplication

$$nP = P + P + \cdots + P$$

- Double and Add algorithm

$$\begin{aligned} 151 &= 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ &= 2^7 + 2^4 + 2^2 + 2^1 + 2^0 \end{aligned}$$

Logarithm



Finite Field $\mathbb{F}_p$

- Operation
  - Addition $(+)$
  - Multiplication $(\cdot)$
- Closed
- Associative and Commutative
- Identity element, Inverse element
- Distributive
- p is a prime number

Finite Field $\mathbb{F}_p$

- Addition: $(18 + 9) \bmod 23 = 4$
- Subtraction: $(7 - 14) \bmod 23 = 16$
- Multiplication: $4 \cdot 7 \bmod 23 = 5$
- Additive inverse: $-5 \bmod 23 = 18$

  Indeed: $(5 + (-5)) \bmod 23 = (5 + 18) \bmod 23 = 0$

- Multiplicative inverse: $9^{-1} \bmod 23 = 18$

  Indeed: $9 \cdot 9^{-1} \bmod 23 = 9 \cdot 18 \bmod 23 = 1$

Division

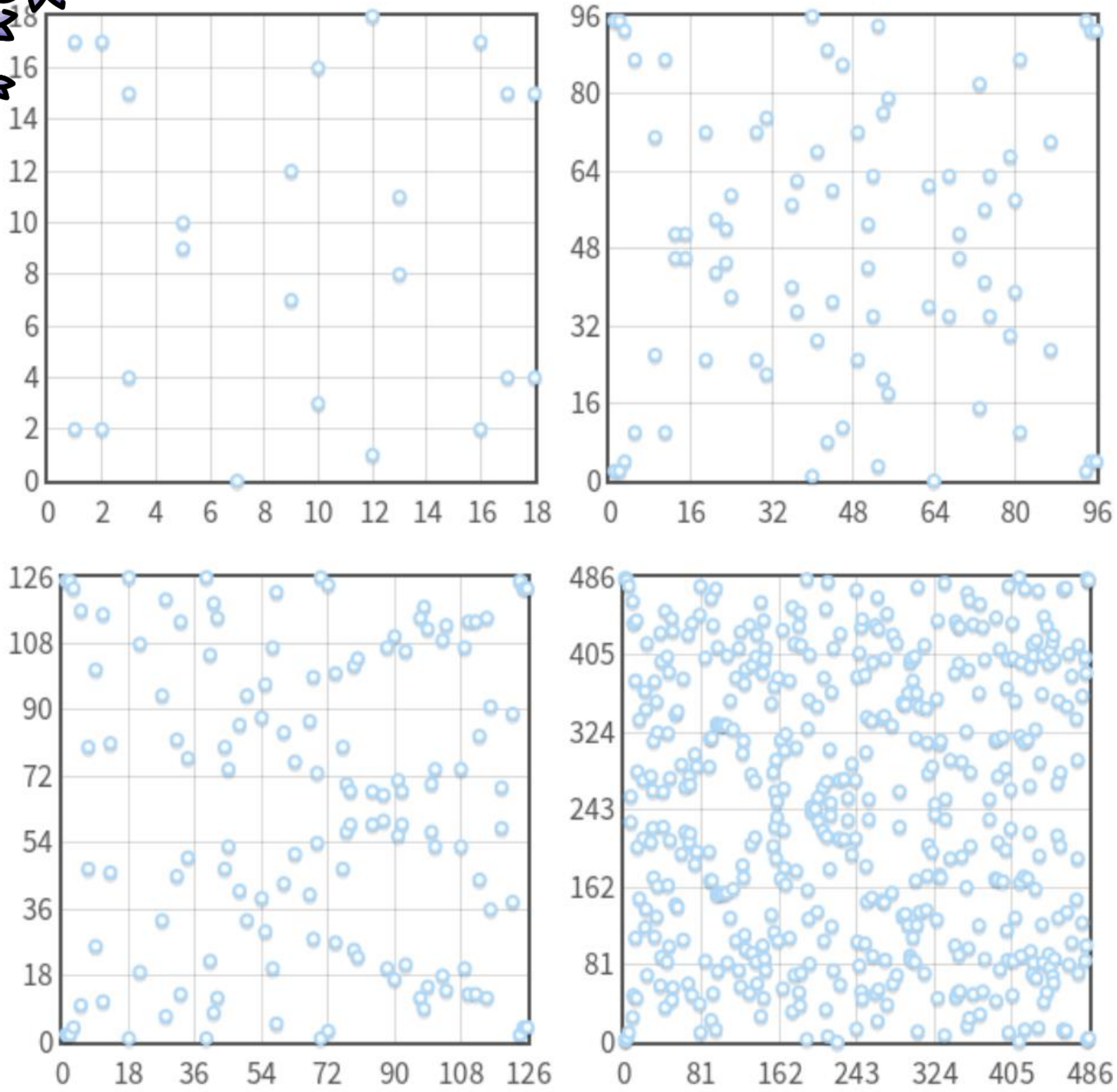
Find inverse and perform multiplication

→ Extended Euclidean Algorithm

Elliptic Curves over $\mathbb{F}_p$

$$\{(x,y) \in \mathbb{R}^2 \quad | \quad y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$

$$\{(x,y) \in (\mathbb{F}_p)^2 \quad | \quad y^2 \equiv x^3 + ax + b \pmod{p},\ 4a^3 + 27b^2 \not\equiv 0 \pmod{p}\} \cup \{0\}$$



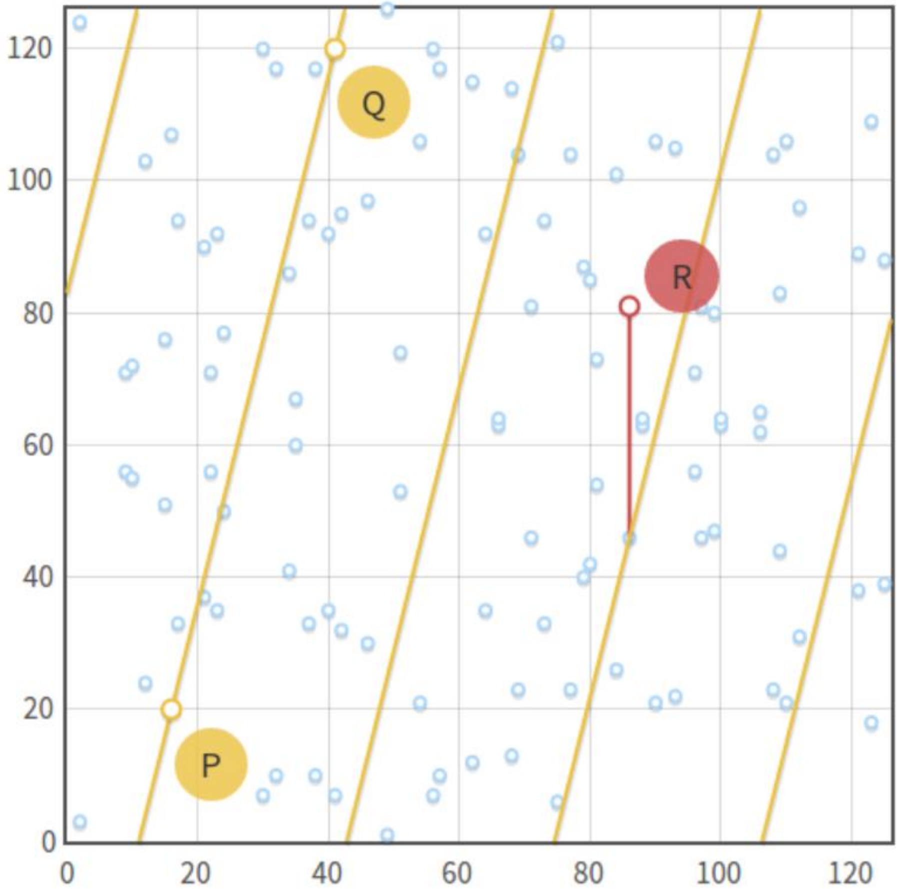
$$y^2 = x^3 - 7x + 10 \ (mod\ p)$$

p = 19, 97, 127, 487

Symmetric

Abelian group

Point Addition



$$P + Q + R = 0, P + Q = -R$$

$P = 0 \; or \; Q = 0$
→Identity element

$P = -Q$
→ Inverse (mod q)

$\cancel{\boldsymbol{P = Q, P \neq Q\ but\ no\ R}}$
~~→ **Tangency (접선) !**~~

Point Addition

$$m = (y_P - y_Q)(x_P - x_Q)^{-1} \bmod p$$

$$\begin{aligned} x_R &= (m^2 - x_P - x_Q) \bmod p \\ y_R &= [y_P + m(x_R - x_P)] \bmod p \\ &= [y_Q + m(x_R - x_Q)] \bmod p \end{aligned}$$

$$m = (3x_P^2 + a)(2y_P)^{-1} \bmod p$$

Order

- Order
    - The number of points

    - Trying all x (from 0 to p-1) is “hard” if p is large

    - Schoof’s algorithm
        - Computing the order

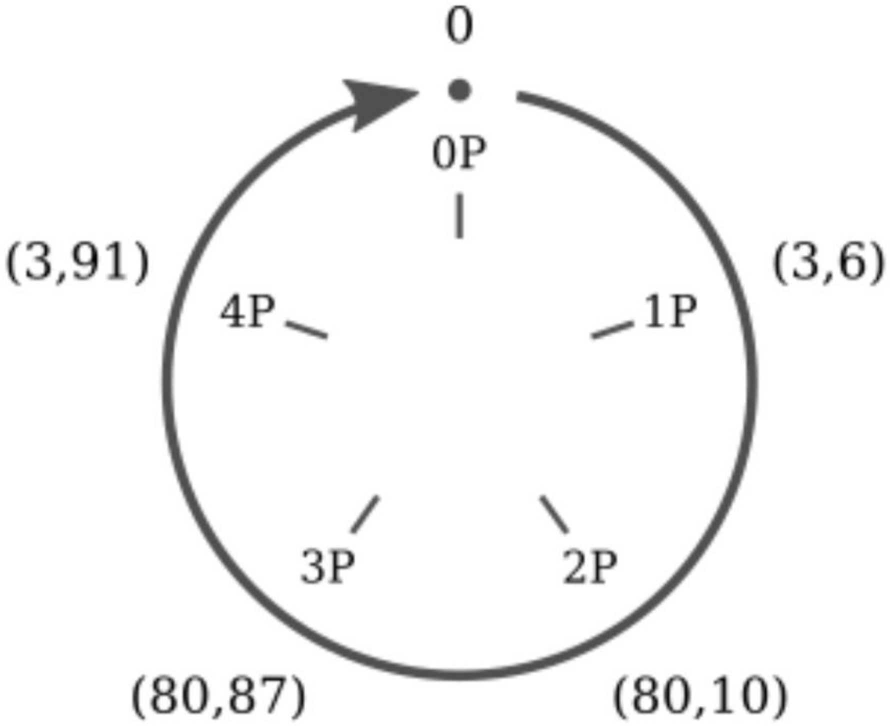
Scalar Multiplication

$$nP = P + P + \cdots + P$$

- Double and Add algorithm

- Cyclic subgroup

$y^2 = x^3 + 2x + 3\ (mod\ 97)\ P = (3,6)$



Scalar Multiplication

- 0P=0
- 1P=(3,6)
- 2P=(80,10)
- 3P=(80,87)
- 4P=(3,91)
- 5P=0
- 6P=(3,6)

…

- 5kP=0
- (5k+1)P=(3,6)
- (5k+2)P=(80,10)
- (5k+3)P=(80,87)
- (5k+4)P=(3,91)

5 points repeated are closed
→Subgroup
P is base point (generator)

Subgroup Order

- Subgroup order
  - Minimum n where nP=0

- Lagrange's theorem
  - The order of subgroup is a divisor or the order of parent group

- Find subgroup order
  - Calculate N
  - Find out all the divisor of N
  - Compute nP
  - Find smallest n such that nP=0

Discrete Logarithm

- Given P and Q, finding k such that Q=kP is “harder”
- No proof, but there is no known polynomial time algorithm
- DSA, DH, ElGamal