Elliptic Curve

→ An Elliptic Curve is a set of points that satisfy the mathematical equation: $y^2 = x^3 + ax + b$ where 'a' and 'b' are some constants with condition $4a^3 + 27b^2 \neq 0$.

⇒ Properties :

→ Elliptic Curve is required to be non-singular.

↳ No cusps / self-intersections.

moving point should not take reverse direction.

→ should satisfy condition: $4a^3 + 27b^2 \neq 0$.

→ An elliptic Curve is an abelian variety.

Example :

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

→ Compare it with

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

$\therefore a = 3$ & $b = 2$

→ check whether given equation is elliptic curve or not.

$$4a^3 + 27b^2 \neq 0$$

$$4(3)^3 + 27(2)^2 \neq 0$$

$$108 + 108 \neq 0$$

$$216 \neq 0$$

$\therefore$ condition satisfied and given equation $y^2 = x^3 + 3x + 2$ is elliptic curve.

(x, y)

→ let point (x, y) be (2, 4)
check whether point (2, 4) is on elliptic curve or not.

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

$4^2 = 2^3 + 3(2) + 2$ ($\because$ put (x, y) = (2, 4) in eq.)

$16 = 8 + 6 + 2$

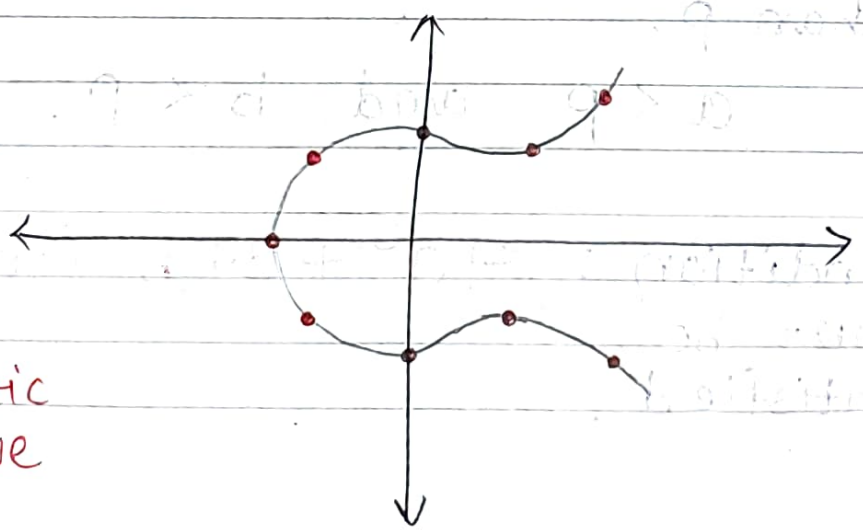
$16 = 16$

$\therefore$ LHS = RHS

$\therefore$ given point (2, 4) is on the elliptic curve $y^2 = x^3 + 3x + 2$.

NOTE: If point (x, y) is on elliptic curve then you will get L.H.S = R.H.S.

If point (x, y) is not on elliptic curve then you will get L.H.S. ≠ R.H.S.



Elliptic Curve

* Elliptic Curve - Types.

1) Elliptic Curve over real numbers.
2) " " " complex "
3) " " " Finite fields.

↳ ex. $y^2 \equiv x^3 + 7 \pmod{17}$

cryptography

Elliptic Curve over Finite Fields

→ finite fields : GF(2), GF(5), GF(8) etc.
Galois field

→ The equation is $E_p(a,b)$ p-prime no.

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

→ value of 'a' and 'b' must be lesser than p.

$a < p$ and $b < p$.

→ Condition : $4a^3 + 27b^2 \pmod{p} \neq 0$ must be satisfied.

Example (1) :

Find all the points on the $E_5(1,1)$.

$\Rightarrow$ $E_5(1,1)$: $\therefore$ $p = 5$ (given)
$E_p(a,b)$ $a = 1$
$b = 1$

$\rightarrow GF(5) = (Z,5) = \{0,1,2,3,4\}$

$0 \bmod 5 = 0$
$1 \bmod 5 = 1$
$2 \bmod 5 = 2$
$3 \bmod 5 = 3$
$4 \bmod 5 = 4$
$5 \bmod 5 = 0$
$6 \bmod 5 = 1$
$7 \bmod 5 = 2$
$8 \bmod 5 = 3$
$9 \bmod 5 = 4$
$10 \bmod 5 = 0$
$11 \bmod 5 = 1$
$12 \bmod 5 = 2$
$13 \bmod 5 = 3$
$14 \bmod 5 = 4$
$15 \bmod 5 = 0$

⋮

GF(5) = {0, 1, 2, 3, 4}

→ The equations :

$$y^2 \equiv x^3 + ax + b \pmod p \longrightarrow (1)$$

$$4a^3 + 27b^2 \pmod p \neq 0 \longrightarrow (2)$$

→ $p = 5$, $a = 1$, $b = 1$ (given) put in (2)

$4a^3 + 27b^2 \pmod p \neq 0$

$4(1)^3 + 27(1)^2 \pmod 5 \neq 0$

$4 + 27 \pmod 5 \neq 0$

$31 \bmod 5 \neq 0$

$1 \neq 0$

∴ $4a^3 + 27b^2 \pmod p \neq 0$

condition satisfied. and given equation $y^2 \equiv x^3 + ax + b \pmod p$ with $E_5(1,1)$ is elliptic curve.

→ put $p = 5$, $a = 1$, $b = 1$ in (1)

$y^2 \equiv x^3 + ax + b \pmod p$

$y^2 \pmod p = x^3 + ax + b \pmod p$

$y^2 \pmod 5 = x^3 + x + 1 \pmod 5$

Elliptic Curve

GF(5)	L.H.S. $y^2 \pmod 5$	R.H.S. $x^3 + x + 1 \pmod 5$
0	$0^2 \bmod 5 = 0$	$0^3 + 0 + 1 \pmod 5 = 1$
1	$1^2 \bmod 5 = 1$	$1^3 + 1 + 1 \pmod 5 = 3$
2	$2^2 \bmod 5 = 4$	$2^3 + 2 + 1 \pmod 5 = 1$
3	$3^2 \bmod 5 = 4$	$3^3 + 3 + 1 \pmod 5 = 1$
4	$4^2 \bmod 5 = 1$	$4^3 + 4 + 1 \pmod 5 = 4$

NOTE: when $\underset{GF(5)}{x = 0}$ then R.H.S. = 1

↳ find GF(5) values where L.H.S. = 1

i.e. L.H.S. = 1 for GF(5) $\rightarrow \overset{y}{1}, \overset{y}{4}$

∴ points are $(\underset{x}{0}, \underset{y}{1})$, $(\underset{x}{0}, \underset{y}{4})$

⇒ The points on the $E_5(1,1)$ are:

(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3).

Example (2) :

Find all the points on the $E_{11}(1,1)$.

$\Rightarrow E_{11}(1,1) \Rightarrow E_p(a,b)$

$\therefore p = 11,\ a = 1,\ b = 1$

$\rightarrow GF(11) = (Z, 11)$

$= \{0,1,2,3,4,5,6,7,8,9,10\}$

$0 \bmod 11 = 0$
$1 \bmod 11 = 1$
$2 \bmod 11 = 2$
$3 \bmod 11 = 3$
$4 \bmod 11 = 4$
$5 \bmod 11 = 5$
$6 \bmod 11 = 6$
$7 \bmod 11 = 7$
$8 \bmod 11 = 8$
$9 \bmod 11 = 9$
$10 \bmod 11 = 10$
$11 \bmod 11 = 0$
$12 \bmod 11 = 1$
$13 \bmod 11 = 2$
$14 \bmod 11 = 3$
$15 \bmod 11 = 4$
$16 \bmod 11 = 5$
$17 \bmod 11 = 6$
$18 \bmod 11 = 7$
$19 \bmod 11 = 8$ .....

GF(11) = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

→ The equations :

$$y^2 \equiv x^3 + ax + b \pmod p \longrightarrow (1)$$

$$4a^3 + 27b^2 \pmod p \neq 0 \longrightarrow (2)$$

→ put $p = 11$, $a = 1$, $b = 1$ in eq. (2)

$$4a^3 + 27b^2 \pmod p \neq 0$$
$$4(1)^3 + 27(1)^2 \pmod{11} \neq 0$$
$$4 + 27 \pmod{11} \neq 0$$
$$31 \bmod 11 \neq 0$$
$$9 \neq 0$$

∴ $4a^3 + 27b^2 \pmod p \neq 0$ condition is satisfied and given equation $E_{11}(1,1)$ is elliptic curve.

→ put $p = 11$, $a = 1$, $b = 1$ in eq. (1)

$$y^2 \equiv x^3 + ax + b \pmod p$$
$$y^2 \pmod p = x^3 + ax + b \pmod p$$

$$\boxed{y^2 \pmod{11} = x^3 + x + 1 \pmod{11}}$$

Elliptic Curve.

GF(11) ↓	L.H.S. $y^2 \pmod{11}$	R.H.S. $x^3+x+1 \pmod{11}$
0	$0^2 \bmod 11 = 0$	$0^3+0+1 \pmod{11} = 1$
1	1	3
2	4	0
3	9	9
4	5	3
5	3	10
6	3	3
7	5	10
8	9	4
9	4	2
10	1	10

$\Rightarrow$ The points on $E_{11}(1,1)$ are :

(0,1), (0,10), (1,5), (1,6), (2,0),
(3,3), (3,8), (4,5), (4,6),
(6,5), (6,6), (8,2), (8,9).

ex: Find all the points on the $E_{13}(3,4)$.

Example ③:

Find all the points on the $E_7(2,3)$.

$\Rightarrow$ $E_7(2,3) \Rightarrow E_p(a,b)$

$\therefore p = 7, \quad a = 2, \quad b = 3$

→ $GF(7) = (Z,7)$

$= \{0,1,2,3,4,5,6\}$

The equations:

$$y^2 \equiv x^3 + ax + b \pmod p \longrightarrow (1)$$

$$4a^3 + 27b^2 \pmod p \neq 0 \longrightarrow (2)$$

→ put $p = 7, a = 2, b = 3$ in eq. (2)

$$4a^3 + 27b^2 \pmod p \neq 0$$
$$4(2)^3 + 27(3)^2 \pmod 7 \neq 0$$
$$4(8) + 27(9) \pmod 7 \neq 0$$
$$275 \bmod 7 \neq 0$$
$$2 \neq 0$$

$\therefore 4a^3 + 27b^2 \pmod p \neq 0$ condition is satisfied and given equation $E_7(2,3)$ is elliptic curve

→ put $p = 7$, $a = 2$, $b = 3$ in eq. (1)

$$y^2 \equiv x^3 + ax + b \pmod p$$

$$y^2 \pmod p = x^3 + ax + b \pmod p$$

$$\boxed{y^2 \pmod 7 = x^3 + 2x + 3 \pmod 7}$$

Elliptic Curve

GF(7) ↓	$y^2 \pmod 7$	$x^3 + 2x + 3 \pmod 7$
0	0	3
1	1	6
2	4	1
3	2	1
4	2	5
5	4	5
6	1	0

⇒ The points on $E_7(2,3)$ are:

(2,1), (2,6), (3,1), (3,6), (6,0).

Example ④

Does the point (3,6) lie on the Elliptic Curve $E_7(2,3)$?

$\Rightarrow$ $y^2 \equiv x^3 + ax + b \pmod p$

$y^2 \pmod p = x^3 + ax + b \pmod p$

→ put $p = 7$, $a = 2$, $b = 3$ (given) in above equation.

$[\because E_7(2,3) \Rightarrow E_p(a,b)$
$\because p = 7, a = 2, b = 3]$

→ $y^2 \pmod p = x^3 + ax + b \pmod p$

$\therefore 6^2 \pmod 7 = 3^3 + 2(3) + 3 \pmod 7$

$[\because$ point $(x,y) = (3,6)]$

$\therefore 36 \bmod 7 = 27 + 6 + 3 \pmod 7$

$\therefore 1 = 36 \bmod 7$

$\therefore 1 = 1$

$\therefore$ L.H.S. = R.H.S.

$\therefore$ given point (3,6) is lies on the Elliptic Curve $E_7(2,3)$.

ex ⑥ point (8,9)
Elliptic Curve $E_{13}(4,5)$.

Example ⑤

Does the point (3,8) lie on the Elliptic Curve $E_{11}(1,1)$?

⇒ $y^2 \equiv x^3 + ax + b \pmod p$

$y^2 \pmod p = x^3 + ax + b \pmod p$

→ put $p = 11$, $a = 1$, $b = 1$ and $x = 3$, $y = 8$ in above eq.

[∵ $E_{11}(1,1) \Rightarrow E_p(a,b)$
∴ $p = 11$, $a = 1$, $b = 1$
∵ point $(x,y) = (3,8)$]

→ $y^2 \pmod p = x^3 + ax + b \pmod p$

∴ $8^2 \pmod{11} = 3^3 + 3(1) + 1 \pmod{11}$

∴ $64 \bmod 11 = 27 + 3 + 1 \pmod{11}$

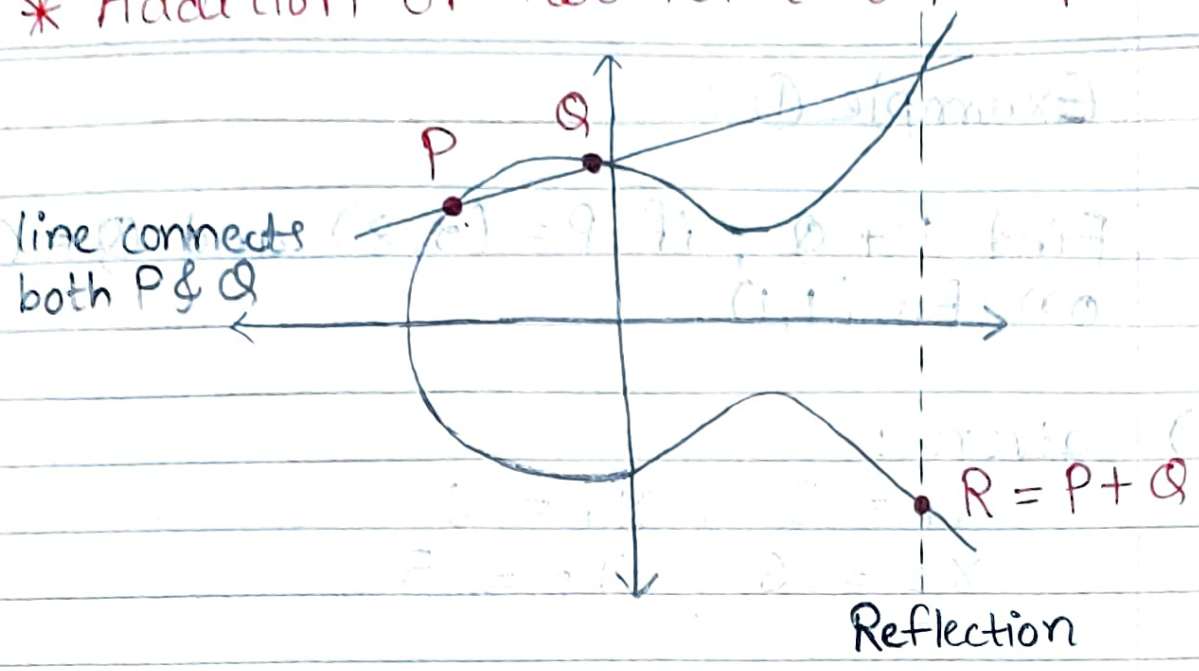
∴ $9 = 31 \bmod 11$

∴ $9 = 9$

∴ L.H.S. = R.H.S.

Hence, the point (3,8) lies on the Elliptic Curve $E_{11}(1,1)$.

* Addition of Two Points on Elliptic Curve



→ Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be in the Elliptic Curve $Ep(a,b)$ and $Q \neq -P$, then the addition over the Elliptic Curve $Ep(a,b)$ is $R(x_3, y_3)$ such that

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$

$$y_3 = \lambda (x_1 - x_3) - y_1 \pmod p$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

↓

slop of the line PQ

→ P & Q are two different points.

Example ① :

Find $P+Q$, if $P=(3,8)$ and $Q=(6,5)$ on $E_{11}(1,1)$.

⟹ given :

$x_1 = 3$, $y_1 = 8$

$x_2 = 6$, $y_2 = 5$

Since $P \neq Q$ and $P \neq -Q$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

$$= \frac{5-8}{6-3} \pmod{11}$$

$$= \frac{-3}{3} \pmod{11} \quad \underline{OR} \quad -3 \times 3^{-1} \bmod 11$$

$$= -1 \bmod 11 \qquad = -3 \times 4 \bmod 11$$

$$= -12 \bmod 11$$

$$\therefore \lambda = 10 \qquad = -1 \bmod 11$$

$$= 10$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$

$$= 10^2 - 3 - 6 \pmod{11}$$

$$\therefore x_3 = 3$$

$$y_3 = \lambda (x_1 - x_3) - y_1 \pmod p$$
$$= 10 (3 - 3) - 8 \pmod{11}$$
$$= -8 \bmod 11$$
$$\therefore y_3 = 3$$

$$\Rightarrow \boxed{R = P + Q = (x_3, y_3) = (3, 3)}$$

P & Q are same points

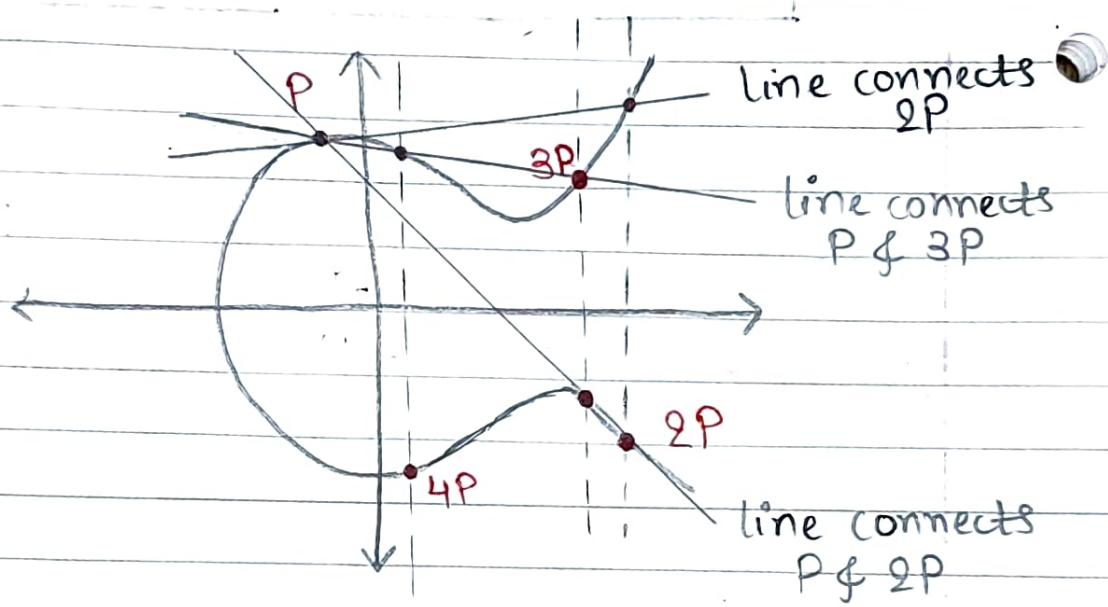
* Addition of two points on Elliptic Curve

→ If P = Q then

$$P + Q = P + P = 2P$$

$$3P = 2P + P$$

$$4P = 3P + P \quad \underline{OR} \quad 2P + 2P$$



→ Let $P = (x_1, y_1)$ and $Q = (x_1, y_1)$ be in the Elliptic Curve $E_p(a, b)$ i.e., $P = Q$, then the addition over the Elliptic Curve $E_p(a, b)$ is $2P(x_3, y_3)$ such that

P and Q are same points.

$$x_3 = \lambda^2 - x - x \pmod p$$

$$y_3 = \lambda (x - x_3) - y \pmod p$$

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

Example ① :

Find $2P$, if $P = (4,6)$ on $E_{11}(1,1)$.

⇒ given : $x = 4$, $y = 6$, $p = 11$, $a = 1$, $b = 1$.

Since $P = Q$,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(4)^2 + 1}{2(6)} \pmod{11}$$

$$= \frac{49}{12} \pmod{11}$$

$$= 49 \times 12^{-1} \pmod{11}$$

$$= 49 \times 1 \pmod{11}$$

$\therefore \lambda = 5$

$$x_3 = \lambda^2 - x - x \pmod p$$
$$= 5^2 - 4 - 4 \pmod{11}$$
$$\therefore x_3 = 6$$

$$y_3 = \lambda (x - x_3) - y \pmod p$$
$$= 5 (4 - 6) - 6 \pmod{11}$$
$$= -16 \bmod 11$$
$$\therefore y_3 = 6$$

$$\Rightarrow \boxed{R = P + P = 2P = (x_3, y_3) = (6, 6)}$$

ex ②: find $2P$, if $P = (3, 6)$ on $E_7(2, 3)$.

$2P = P + P$
$3P = 2P + P$
$4P = 3P + P$ or $2P + 2P$ .....

Example ① :

Find $3P$, if $P = (4,6)$ on $E_{11}(1,1)$.

$\Rightarrow$ $2P + P = 3P$

→ Find $2P$ using formulas of $P = Q$

for answer of $2P$: refer previous example

$2P = (6,6)$

→ given $P = (4,6)$

Add $2P$ & P using formulas of $P \neq Q$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

$$= \frac{6-6}{4-6} \pmod{11}$$

$$= 0 \bmod 11$$

$\therefore \lambda = 0$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$
$$= 0^2 - 6 - 4 \pmod{11}$$

$$\therefore x_3 = 1$$

$$y_3 = \lambda (x_1 - x_3) - y_1 \pmod p$$
$$= 0\,(6-1) - 6 \pmod{11}$$
$$= -6 \bmod 11$$

$$\therefore y_3 = 5$$

$$\Rightarrow \boxed{R = 2P + P = 3P = (x_3, y_3) = (1, 5)}$$

ex (2) : find $3P$, if $P = (3, 6)$ on $E_7(2, 3)$.

* Properties of Elliptic Curve over Finite Fields

→ Consider the elliptic curve E such that the points on the elliptic curve over a finite field F_p, $E(F_p)$, is a finite abelian group.

① Closure

→ If $P \in E(F_p)$ and $Q \in E(F_p)$, then $P + Q \in E(F_p)$.

② Associativity

→ If $P \in E(F_p)$, $Q \in E(F_p)$ and $R \in E(F_p)$, then

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

③ Identity

→ If $P \in E(F_p)$, there exist an identity element which is the point at infinity O, such that

$$P + O = O + P = P.$$

④ Additive Inverse

→ If $P \in E(F_p)$, then every point P has an inverse $P' \in E(F_p)$ such that

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

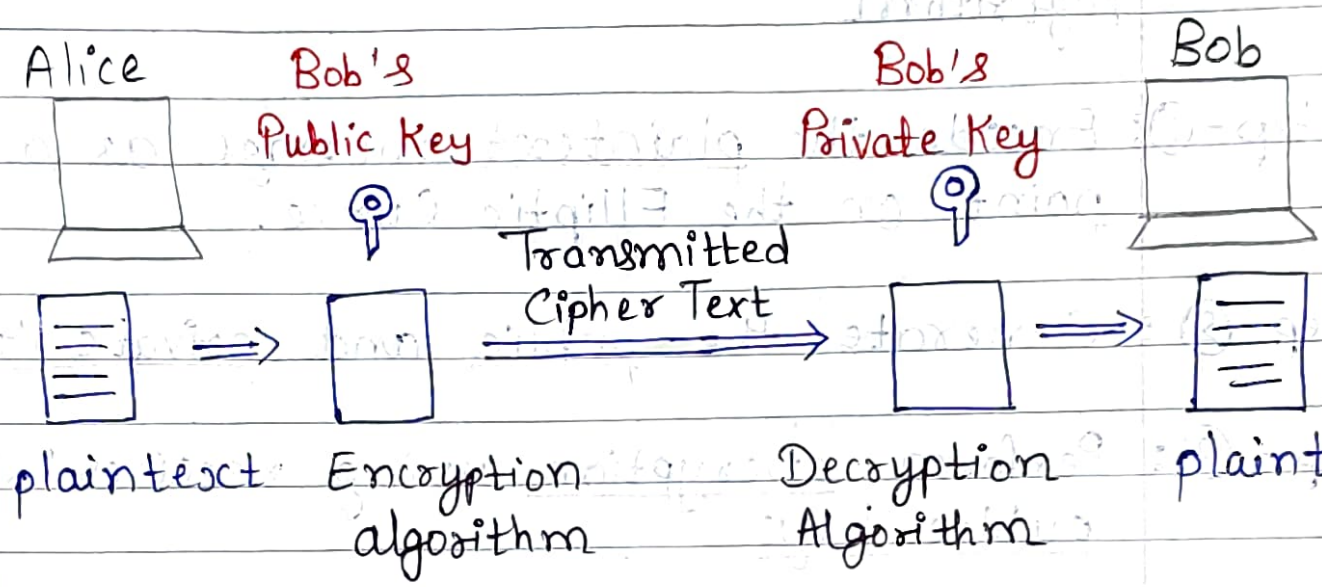
⑤ Commutative

→ If $P \in E(F_p)$ and $Q \in E(F_p)$, then

$$P + Q = Q + P.$$

⇒ $E(F_p)$ is called as finite abelian group because it is following the properties Closure, Associativity, Identity, Additive Inverse and Commutative properties.

Public Key Cryptography



* Elliptic Curve Cryptography

Algorithm

Step-①: Encode the plaintext message as a point on the Elliptic Curve.

Step-②: Generate the public and private keys.

step-③: Perform encryption using receiver's public keys.

step-④: Decrypt the message using receiver's private key.

Step-①: Elliptic Curve = $Ep(a,b)$

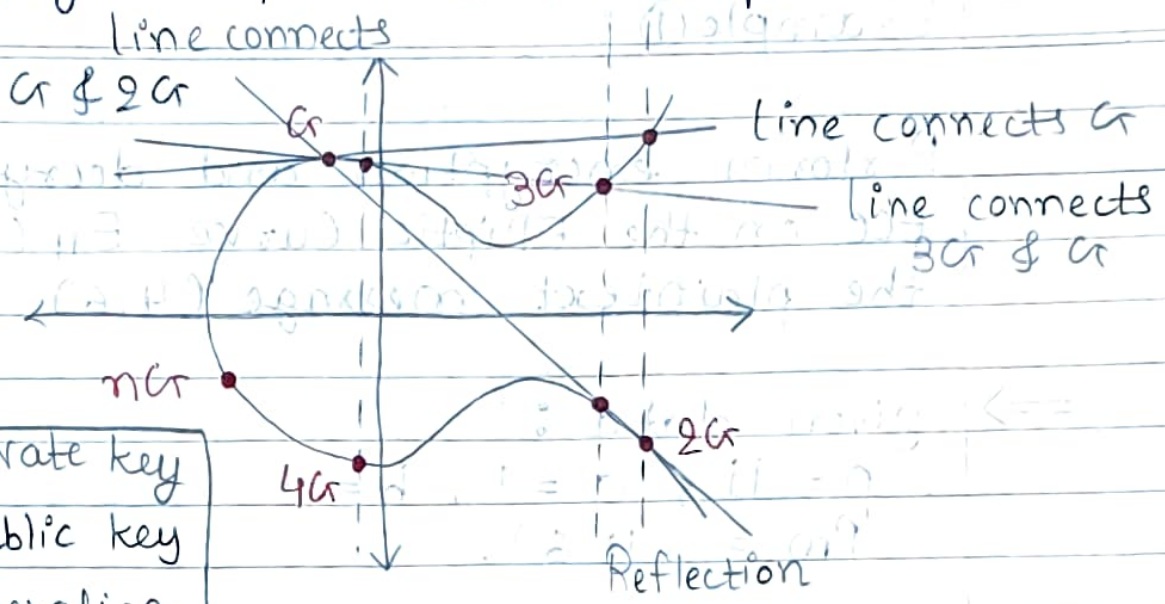
Plaintext $Pm = (x, y)$

Step-②: Let $G = (x, y) \in Ep(a,b)$.
generator point

Select **Private Key = n**

Compute **Public Key (PU) = nG**

→ Adding two points on the Elliptic Curve



n - private key
nG - Public key
G - Generating Point

Step-②: Ciphertext $C = (C_1, C_2)$

$C_1 = kG$

where G = generator point
k = random number, $1 < k < p-1$
p = large prime number

$C_2 = P_m + kPU$

public key $PU = nG$.

$\Rightarrow C = (C_1, C_2)$

$$\boxed{C = (kG, (P_m + kPU))}$$

Step-④: given Ciphertext $C = (C_1, C_2)$ & Private key n

Plaintext

$$\boxed{P_m = C_2 - nC_1}$$

Example ① :

Perform encryption and decryption using ECC on the Elliptic Curve $E_{11}(1,1)$ with the plaintext message (4,6).

$\Rightarrow$ given data :

$p = 11,\ a = 1,\ b = 1$

$P_m = (4,6)$.

→ Generate the public and private keys.

Let $G = (1,5) \in E_{11}(1,1)$

select private key $n = 2$

Compute public key

$$PU = nG$$

$$\therefore PU = 2G \quad [\because \text{take } n = 2]$$

Compute $2G = 2(1,5)$

$x \quad y$

Since $P = Q$,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(1)^2 + 1}{2(5)} \pmod{11}$$

$$= \frac{4}{10} \pmod{11}$$

$$= 4 \times 10^{-1} \pmod{11}$$

$$\lambda = 4 \times 10 \mod 11$$

$$\therefore \lambda = 7$$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 7^2 - 1 - 1 \pmod{11}$$

$$\therefore x_3 = 3$$

$$y_3 = \lambda (x - x_3) - y \pmod p$$

$$= 7 (1-3) - 5 \pmod{11}$$

$$= -19 \mod 11$$

$$\therefore y_3 = 3$$

→ Public key $PU = 2G = (x_3, y_3)$

$\therefore PU = (3,3)$

Private key $n = 2$ [∵ selected]

→ Perform encryption using receiver's public key.

Ciphertext $C = (kG, (Pm + kPU))$

Let $k = 2$

$$C = (\underline{2(1,5)}, ((4,6) + \underline{2(3,3)}))$$

$P = Q$ (for $2(1,5)$)

$P = Q$ (for $2(3,3)$)

$P \neq Q$ (for $(4,6) + 2(3,3)$)

x y

→ for 2(3,3)

since P = Q,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(3)^2 + 1}{2(3)} \pmod{11}$$

$$= \frac{28}{6} \pmod{11}$$

$$= \frac{14}{3} \pmod{11}$$

$$= 14 \times 3^{-1} \pmod{11}$$

$$= 14 \times 4 \pmod{11}$$

$$\therefore \lambda = 1$$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 1^2 - 3 - 3 \pmod{11}$$

$$= -5 \bmod 11$$

$$\therefore x_3 = 6$$

$$y_3 = \lambda(x - x_3) - y \pmod p$$

$$= 1(3 - 6) - 3 \pmod{11}$$

$$= -6 \bmod 11$$

$$\therefore y_3 = 5$$

→ ∴ 2 (3,3) = (x_3, y_3)

∴ 2 (3,3) = (6,5)

→ C = (2 (1,5), ((4,6) + (6,5))) (2(3,3); P ≠ Q)

for (4,6) + (6,5) (x_1 y_1 x_2 y_2)

Since P ≠ Q,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

$$= \frac{5-6}{6-4} \pmod p$$

$$= \frac{-1}{2} \bmod 11$$

$$= -1 \times 2^{-1} \bmod 11$$

$$= -1 \times 6 \bmod 11$$

$$= -6 \bmod 11$$

∴ $\lambda = 5$

$$X_3 = \lambda^2 - X_1 - X_2 \pmod p$$

$$= 5^2 - 4 - 6 \pmod{11}$$

$$= 15 \bmod 11$$

∴ $X_3 = 4$

$$y_3 = \lambda (x_1 - x_3) - y_i \pmod p$$
$$= 5 (4-4) - 6 \pmod{11}$$
$$= -6 \bmod 11$$
$$\therefore y_3 = 5$$

→ $\therefore (4,6) + (5,5) = (x_3, y_3) = (4,5)$

→ $C = (2(1,5), ((4,6) + (6,5)))$

$= (2(1,5), (4,5))$

$P = Q$

$x \quad y$

→ for $2(1,5)$

since $P = Q$,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$
$$= \frac{3(1)^2 + 1}{2(5)} \pmod{11}$$
$$= 4 \times 10^{-1} \pmod{11}$$
$$= 4 \times 10 \bmod 11$$
$$= 40 \bmod 11$$
$$\therefore \lambda = 7$$

$$x_3 = \lambda^2 - x - x \pmod p$$
$$= 7^2 - 1 - 1 \pmod{11}$$
$$\therefore x_3 = 3$$

$$y_3 = \lambda (x - x_3) - y \pmod p$$
$$= 7 (1-3) - 5 \pmod{11}$$
$$= -19 \bmod 11$$
$$\therefore y_3 = 3$$

→ $\therefore 2(1,5) = (x_3, y_3) = (3,3)$

→ $C = (2(1,5), (4,5))$
$\therefore C = ((3,3), (4,5))$

→ Decrypt the message using private key.

Plaintext $Pm = C_2 - nC_1$

given $C = (C_1, C_2) = ((3,3), (4,5))$
$C_1 = (3,3)$ & $C_2 = (4,5)$

$\therefore Pm = (4,5) - \underbrace{2(3,3)}_{P = Q}$ $[\because n = 2]$

$\overset{x}{} \quad \overset{y}{}$

→ for $2(3,3)$

since $P = Q$,

$$\lambda = \frac{3x^2 + a}{2y} \pmod{11}$$

$$= \frac{3(3)^2 + 1}{2(3)} \pmod{11}$$

$$= \frac{28}{6} \bmod 11$$

$$= \frac{14}{3} \bmod 11$$

$$= 14 \times 3^{-1} \bmod 11$$

$$= 14 \times 4 \bmod 11$$

$\therefore \lambda = 1$

$$x_3 = \lambda^2 - x - x \pmod{p}$$

$$= 1^2 - 3 - 3 \pmod{11}$$

$$= -5 \bmod 11$$

$\therefore x_3 = 6$

$$y_3 = \lambda(x - x_3) - y \pmod{p}$$

$$= 1(3 - 6) - 3 \pmod{11}$$

$$= -6 \bmod 11$$

$\therefore y_3 = 5$

$\therefore 2.(3,3) = (x_3, y_3) = (6,5)$

$\Rightarrow \therefore Pm = (4,5) - 2(3,3)$

$= (4,5) - (6,5)$

$= (4,5) + (6,-5)$

$= (4,5) + (6,6)$ $[\because -5 \bmod 11 = 6]$

$P \neq Q$

Since $P \neq Q$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

$$= \frac{6-5}{6-4} \pmod{11}$$

$$= \frac{1}{2} \bmod 11$$

$$= 1 \times 2^{-1} \bmod 11$$

$$= 1 \times 6 \bmod 11$$

$\therefore \lambda = 6$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$

$$= 6^2 - 4 - 6 \pmod{11}$$

$$= 26 \bmod 11$$

$\therefore x_3 = 4$

$$y_3 = \lambda (x_1 - x_3) - y_1 \pmod p$$
$$= 6 (4-4) - 5 \pmod{11}$$
$$= -5 \bmod 11$$
$$\therefore y_3 = 6$$

$\therefore (4,5) + (6,6) = (x_3, y_3) = (4,6)$

$Pm = (4,5) + (6,6)$

$\therefore \boxed{Pm = (4,6)}$