MODULE - 5

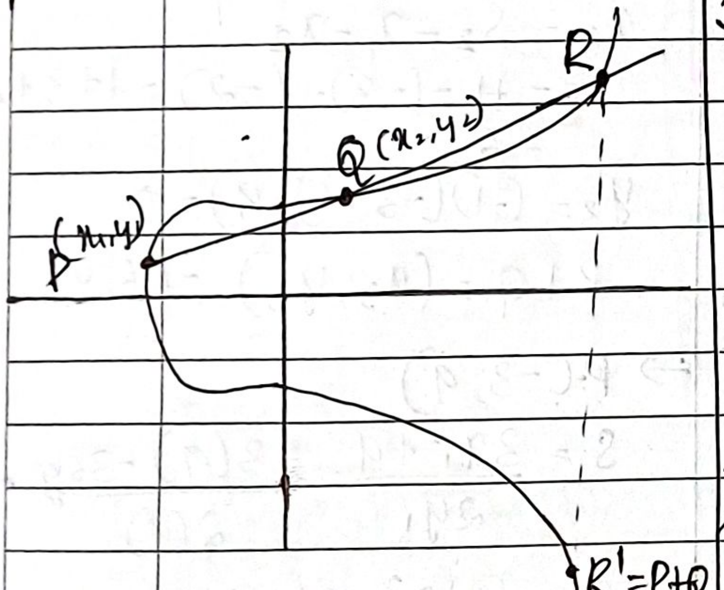
13/11/24 **Elliptic curves and Elliptic Curve Cryptography**

Elliptic curve: An elliptic curve is a graph E or E(a,b) of an equation $y^2 = x^3 + ax + b$ where x, y, a and b are real numbers or rational no. or integer modulo $m > 1$. [$x, y, a, b \in \mathbb{R}, \mathbb{Q}, \mathbb{F}_p$]

The set E contains a point at infinity denoted by O [point at ∞]

→ For a given eq, the discriminant $4a^3 + 27b^2 \neq 0$

↳ This implies that the elliptic curve does not have a repeated root, thus we are excluding elliptic curve which have a double point or a cusp



→ **Observations**:-

1) Elliptic curve are symmetric above x-axis.

2) If $P = (x, y)$ lies on the graph $y^2 = x^3 + ax + b$, we define $-P$ as $(x, -y)$ [$-P = (x, -y)$], i.e $-P$ is 'P' reflected in the x axis

3) Give 2 points p and q on the graph and on the same vertical line, then they must have the form $(x, \pm y)$ that is $Q = -P$ and we define $P + Q = O$ & the identity element of the group

4) Also if $P + O = O + P = P$, for any element p of the elliptic curve.

5) To add a point $P \neq O$ to itself, draw the tangent line that is vertical then $\boxed{P = (x, 0)}$ [∵ as $y = 0$] Imp

and we define $P + P = O$

6) If the tangent line is not vertical then it intersects the graph in exactly one more point say R and we define $P + P = -R$

7) If we consider two points

say P and Q $(P \neq Q)$. draw a straight line joining P and Q, that line intersects the third point R on the elliptic curve

• Reflection of R is P+Q

i.e $P+Q=-R$,

$$\boxed{P+Q+R=0}$$

⇒ An elliptic curve E with addition operator + forms an abelian group with identity element 'O' and the inverse of P is −P

(i) $P+Q \in E$, $\forall P, Q \in E$

(ii) $P+O=O+P=P$, $\forall P \in E$

(iii) $(P+Q)+R = P+(Q+R)$, $\forall P, Q, R \in E$

(iv) $P+P=O$ then $-P$ is inverse of P.

$P=(x,y)$ then $-P=(x,-y)$

(v) $P+Q=Q+P$, $\forall P, Q \in E$

Formula for Coordinates of P+Q

Let E be defined by $y^2=x^3+ax^2+b$, let $P=(x_1,y_1)$ and $Q=(x_2,y_2)$.

Then $P+Q=(x_3,y_3)$ where $(P \neq Q)$

$$\boxed{x_3=S^2-x_1-x_2}$$

$$\boxed{y_3=S(x_1-x_3)-y_1}$$

where S is the slope of the line joining P and Q

$$\boxed{S=\frac{y_2-y_1}{x_2-x_1}}$$

⇒ when $P=Q$ or $2P$, where

$$\boxed{x_3=S^2-2x_1}$$

$$\boxed{y_3=-y_1+S(x_1-x_3)}$$ where

$$\boxed{S_3=\frac{3x_1^2+a}{2y_1}}$$

19/4/24

→ On the elliptic curve $y^2=x^3-36x$, let $P=(-3,9)$ and $Q=(-2,8)$. Find P+Q and 2P

Ans $a=-36$
$b=0$

$$S_2=\frac{y_2-y_1}{x_2-x_1}=\frac{8-9}{-2+3}=-1$$

$$x_3=S_2-x_1-x_2$$
$$=1-(-3)-(-2)=1+3+2$$
$$=6$$

$$y_3=(-1)(-3-6)-9)=0$$

$$P+Q=(x_3,y_3)=(6,0)$$

→ $P=(-3,9)$

$$S=\frac{3x_1^2+a}{2y_1}=\frac{3(9)-36}{2(9)}=\frac{-1}{2}$$

$$x_3=\left(\frac{-1}{2}\right)^2-2(-3)=\frac{25}{4}$$

$$y_3=-9+\left(\frac{-1}{2}\right)\left(-3-\frac{25}{4}\right)$$
$$=\frac{-35}{8}$$

2) On the elliptic curve $y^2 = x^3 + 8$, compute $P + P_1$ where $P = (1, 3)$

ans $x_3 = s^2 - 2x_1$; $a = 0$, $x_1 = 1$, $y_1 = 3$

$$S = \left(\frac{3x_1^2 + a}{2y_1}\right)$$

$$S = \frac{3*(1)^2 + 0}{2(3)} = \frac{3}{6} = \frac{1}{2}$$

$$x_3 = s^2 - 2x_1 = \left(\frac{1}{2}\right)^2 - 2(1)$$

$$x_3 = \frac{1}{4} - 2 = \frac{-7}{4}$$

$$\Rightarrow y_3 = -y_1 + s(x_1 - x_3)$$

$$= -3 + \frac{1}{2}\left(1 - \left(-\frac{7}{4}\right)\right)$$

$$= -3 + \frac{1}{2}\left(\frac{4+7}{4}\right)$$

$$y_3 = \frac{-24 + 11}{8} = \frac{-13}{8}$$

$$\underline{2P = \left(\frac{-7}{4}, \frac{-13}{8}\right)}$$

If asked for 4p then consider $2p = \left(\frac{-7}{4}, \frac{-13}{8}\right)$ and recompute x_1 y_1

$\Rightarrow$ Elliptic Curves on Integer modulo n

- If a and b ~~under~~ and the coordinates of points say P and Q on the elliptic curve $E_{a,b}$ are integers mod n then the coordinates of P+Q will be integers modulo m.

The modulus m cannot be even because we have to divide by 2 in the formula for the slope S when P=Q.

- The condition on the discriminent becomes $\boxed{4a^3 + 27b^2 \not\equiv 0 \pmod m}$

Ex: Let us look at the points of the elliptic curve $y^2 \equiv x^3 + 3x + 4 \pmod 7$

x	$x^3+3x+4 \pmod 7$	$y^2 \equiv 4 \pmod 7$ y
$x=0$	4	2,5
$x=1$	1	1,6
$x=2$	4	2,5
$x=3$	5	none
$x=4$	3	none
$x=5$	4	2,5
$x=6$	0	0

$\rightarrow y^2 \equiv 4 \pmod 7 \Rightarrow 2, 5$

$\rightarrow y^2 \equiv 1 \pmod 7 \Rightarrow 1, 6$

$\rightarrow y^2 \equiv 0 \pmod 7 \Rightarrow 0$

$\rightarrow$ Points of the elliptic curve $y^2 \equiv x^3 + 3x + 4 \pmod 7$ are (0,2) (0,5), (1,1), (1,6), (2,2) (2,5) (5,2), (5,5) (6,0), O. [x and y]

20/11/24

→ On the elliptic curve $y^2 \equiv x^3 + 3x + 4 \pmod 7$ let $P = (1,1)$ & $Q = (2,5)$ find $P+Q$ & double the point $R = (2,2)$

ans $P = (1,1)$ and $Q = (2,5)$

$x_1 = 1$; $y_1 = 1$; $x_2 = 2$; $y_2 = 5$

$\therefore P+Q = (\underset{x_3}{?}, \underset{y_3}{?})$ $a = 3$

$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

$x_3 = \left(\frac{4}{2-1}\right)^2 - 1 - 2 = 16 - 3 = 13$

$13 \equiv 6 \pmod 7$

$\boxed{x_3 = 6}$

→ $y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \pmod 7$

$= 4(1-6) - 1 \pmod 7$

$= 4(-5) - 1$

$= -21 \equiv 0 \pmod 7$

$\boxed{y_3 = 0}$

$\therefore P+Q = (6,0)$

$R = (\overset{x_1}{2}, \overset{y_1}{2})$

$2R = (x_3, y_3)$

$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$

$= \left(\frac{3(2)^2 + 3}{2(2)}\right)^2 - 2(2)$

$x_3 = \cancel{(3)^2 - 2 = 7}\ \left(\frac{15}{4}\right)^2 - 4 = \frac{161}{16}$

$\cancel{y_3 = -y_1 + s(x_1 - x_3)}$

$\cancel{= -1 + \left(\frac{3(1)^2 + 3}{2(1)}\right)(1-8)}$

$\cancel{y_3 = -2 + 3(2}$

$x_3 = \frac{161}{16} \pmod 7$

$= 161 \cdot 16^{-1} \pmod 7$

$= 161 \cdot 1 \equiv 0 \pmod 7$

$\boxed{x_3 = 0}$

→ $y_3 = -y_1 + s(x_1 - x_3)$

$= -2 + \frac{15}{4}(2-0)$

$y_3 = -2 + \frac{15}{2} = \frac{11}{2} \equiv \frac{4}{2} \pmod 7$

$\boxed{y_3 = 2}$

$\boxed{2R = (0,2)}$

20/11/24

→ On elliptic curve $y^2 = x^3 + 5x + 2 \pmod{11}$, let $P = (2, 3)$, $Q = (4, 3)$. Find $P+Q$, $2P$ and $2Q$.

ans $a = 5$

$x_1 = 2 \quad x_2 = 4$

$y_1 = 3 \quad y_2 = 3$

$P + Q = (x_3, y_3)$

$x_3 = s^2 - x_1 - x_2$

$y_3 = s(x_1 - x_3) - y_1$

→ $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 2 - 4$

$= 0 - 6 = -6 \pmod{11}$

$= 5 \pmod{11}$ $\boxed{x_3 = 5}$

→ $y_3 = 0(2-4) - 3$

$y_3 = -3 \equiv 8 \pmod{11}$ $\boxed{y_3 = 8}$

$P+Q$ $(5, 8)$

$P = (2, 3)$

$2P = (x_3, y_3)$

$s_3 = \frac{3x_1^2 + a}{2y_1} = \frac{3(2)^2 + 5}{2(3)}$

$s_3 = \frac{17}{6} \equiv \frac{6}{6} \pmod{11} = 1$ $\boxed{s_3 = 1}$

$x_3 = s^2 - 2x_1 = \left(\frac{17}{6}\right)^2 - 2(2)$

$= \frac{145}{36} \equiv 5 \pmod{11}$

$x_3 = 1^2 - 2(2) = -3 \pmod{11}$

$\boxed{x_3 = 8}$

$y_3 = -y_1 + s(x_1 - x_3)$

$= -3 + 1(2 - 8)$

$= -3 - 6 = -9 \equiv 2 \pmod{11}$

$\boxed{y_3 = 2}$

$2P = (8, 2)$

For $2Q$

$Q = (4, 3)$

$\Rightarrow x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$

$= \left(\frac{17}{6}\right)^2 - 4 = \frac{289}{36} - 4$

$= \frac{145}{36} \equiv \frac{2}{3} \pmod{11}$

$x_3 = 2 \cdot 3^{-1}$

$3 \cdot 3^{-1} \equiv 1 \pmod{11}$

$12 \equiv 1 \pmod{11}$ ✓

$\boxed{3^{-1} = 4}$

$\Rightarrow x_3 = 2 \cdot 4 = 8 \pmod{11}$

$\boxed{x_3 = 8}$

$\Rightarrow y_3 = -y_1 + s(x_1 - x_3)$

$= -3 + \frac{17}{6}(2 - 8)$

$= -3 - 17 = -20$

$y_3 = -20 \pmod{11} = 2$

$\boxed{y_3 = 2}$

$2Q \Rightarrow Q = (4, 3)$ (x_1, y_1)

$x_3 = \left(\frac{3(4)^2 + 5}{2(3)}\right)^2 - 2(4)$

$= \left(\frac{53}{6}\right)^2 - 8$

$x_3 = \frac{2521}{36} \equiv \frac{2}{3} \pmod{11}$

$\boxed{x_3 = 8}$

$$y_3 = -y_1 + s(x_1 - x_3)$$
$$= -3 + \frac{53}{6}(4-8)$$
$$= -3 + \frac{53}{6}(-4)$$
$$= \frac{-115}{3} \equiv \frac{6}{3} \pmod{11}$$
$$= 2 \pmod{11}$$

$\boxed{y_3 = 2}$ $2Q = (8, 2)$

Theorem: Hasse Theorem

- Let the elliptic curve E modulo a prime p have 'N' points then
$p+1 - 2\sqrt{p} \le N \le p + 1\ 2\sqrt{p}$