Operation over E

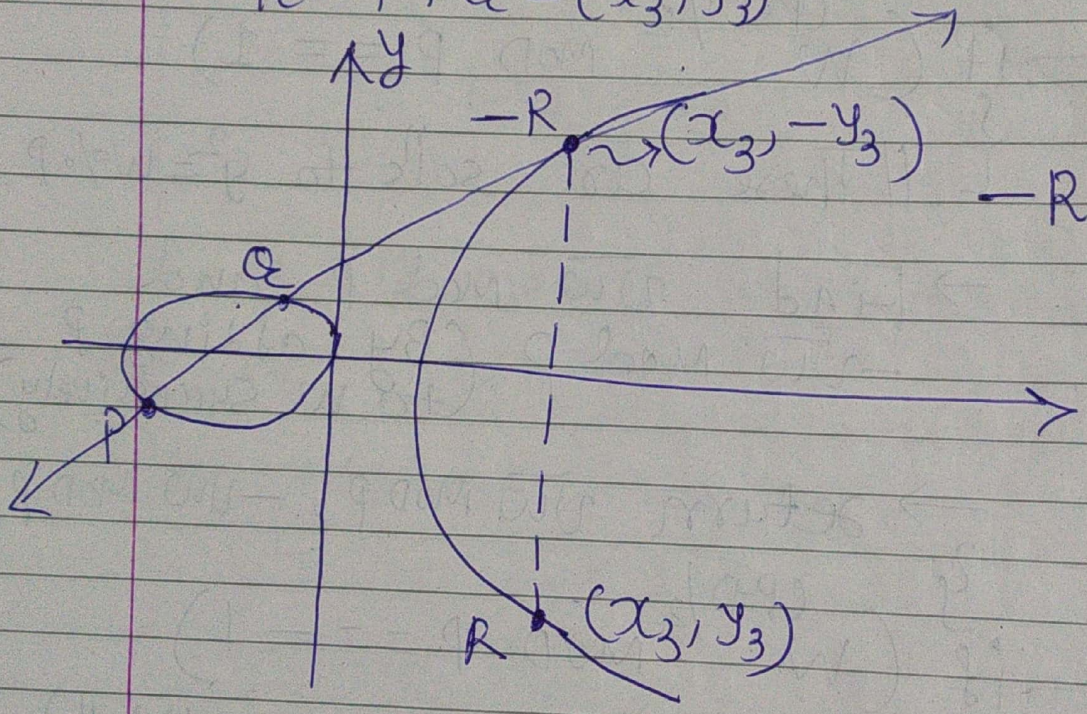
→ E : Set of points over curve $E_p(a,b)$

Operator : +

→ Defⁿ of + ÷

Case 1 : $P=(x_1, y_1)$, $Q=(x_2, y_2)$ } Points over $E_p(a,b)$

$R = P + Q = (x_3, y_3)$



-R : Reflection of R

Slope of line joining Points P, Q

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

Line Joining P and Q also intersects the curve $E_p(a,b)$ at $-R = (x_3, -y_3)$

We know that

$$y - y_1 = \lambda (x - x_1)$$ (Slope point equation)

↳ ①

→ Eq. ① (Line has point -R) satisfies

$$-y_3 - y_1 = \lambda (x_3 - x_1)$$ ($\because (x_3, -y_3)$ is on the Line)

$$\therefore y_3 + y_1 = -\lambda (x_3 - x_1)$$

$$\therefore y_3 = -\lambda (x_3 - x_1) - y_1$$

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

Since $(x_3, -y_3) \in E_p(a, b)$, it also satisfies

$$y_3^2 = (x_3^3 + a x_3 + b) \text{ MOD } p$$

$$\therefore [\lambda (x_1 - x_3) - y_1]^2 = x_3^3 + a x_3 + b$$

$$\therefore \lambda^2 (x_1^2 - 2 x_1 x_3 + x_3^2) - 2\lambda y_1 (x_1 - x_3) + y_1^2 = x_3^3 + a x_3 + b$$

$$\therefore \lambda^2 x_1^2 - 2\lambda^2 x_1 x_3 + \boxed{\lambda^2 x_3^2} - 2\lambda x_1 y_1 + 2\lambda x_3 y_1 + y_1^2 = (x_3^3) + a x_3 + b$$

$$\therefore x_3^3 - \lambda^2 x_3^2 + a x_3 + 2\lambda^2 x_1 x_3 - 2\lambda x_3 y_1 + b - \lambda^2 x_1^2 + 2\lambda x_1 y_1 - y_1^2 = 0$$

If I think it as polynomial of degree 3 and say we rewrite it as

$$\therefore \underline{x^3 - \lambda^2 x^2 + ax + 2\lambda^2 x_1 x - 2\lambda x y_1} + \underline{b - \lambda^2 x_1^2 + 2\lambda x_1 y_1 - y_1^2 = 0} \quad \text{(put } x \text{ in place of } x_3\text{)}$$

$\Rightarrow$ (A)

If we say the sol^{n}s of this Poly. equation as α, β, γ then

$$\alpha + \beta + \gamma = \frac{-(\text{coefficient of } x^2)}{\text{coefficient of } x^3}$$

$$\left(\text{i.e. } \frac{-b}{a}\right)$$

$$= \frac{-(-\lambda^2)}{1}$$

$$= \lambda^2$$

$$\therefore \alpha + \beta + \gamma = \lambda^2 \Rightarrow \gamma = \lambda^2 - \alpha - \beta$$

Since (x_1, y_1), (x_2, y_2), (x_3, y_3) $\in E_p(a, b)$

$x_1 + x_2 + x_3 = \lambda^2$ ($\because$ all x_1, x_2, x_3 can satisfy ⊛)

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

In short, if $P \neq Q$ then

$R = P + Q = (x_3, y_3)$

where

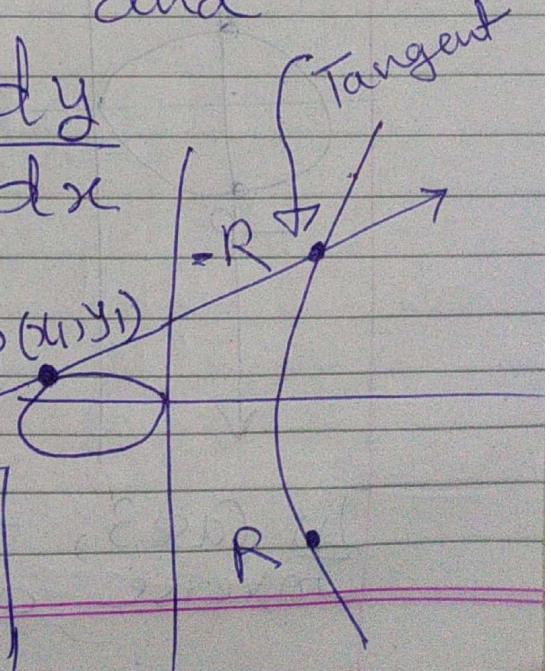
$$x_3 = (\lambda^2 - x_1 - x_2) \text{ MOD } P$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \text{ MOD } P$$

Case 2: If $P = Q = (x_1, y_1)$

then line will be tangent to the curve and

slope of tangent $= \frac{dy}{dx}$



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

$\therefore 2y \frac{dy}{dx} = 3x^2 + a$

$$\therefore \boxed{\left(\frac{dy}{dx}\right)_{(x_1, y_1)} = \frac{3x_1^2 + a}{2y_1} = \lambda}$$

In Case 2, $P = Q$

$\therefore P + Q = P + P$

$= 2P = R = (x_3, y_3)$

where $x_3 = \lambda^2 - x_1 - x_2 = \lambda^2 - 2x_1$

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

$\therefore$ If $P = Q = (x_1, y_1)$

$R = P + Q = P + P = 2P = (x_3, y_3)$

where

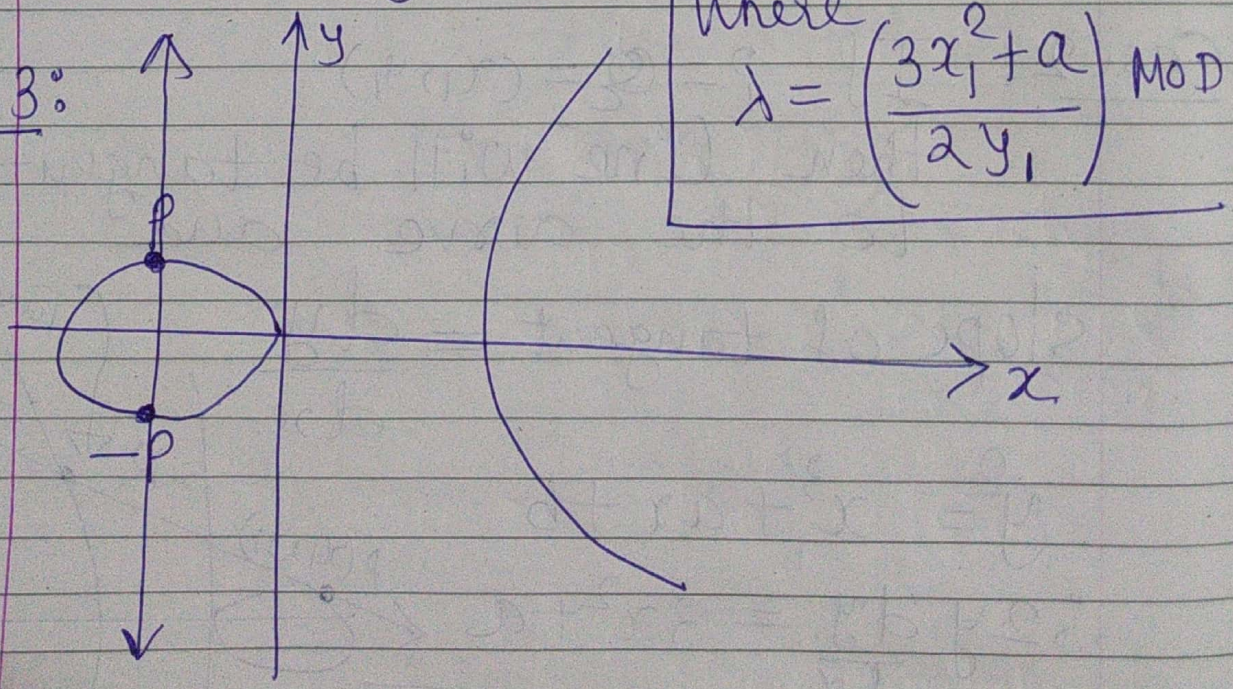
$x_3 = (\lambda^2 - 2x_1) \text{ MOD Prime } P$

$y_3 = [\lambda(x_1 - x_3) - y_1] \text{ MOD Prime } P$

where

$\lambda = \left(\frac{3x_1^2 + a}{2y_1}\right) \text{ MOD Prime}$

Case 3:



In Case 3, two points are additive Inverse of each other.

If $P=(x_1, y_1)$, the second point is $Q=(x_1, -y_1)$ i.e. $Q=-P$

Line Joining P and Q doesn't intersect the curve at third point.

Mathematicians say that the Intercepting point is at ∞; they define a point $\mathcal{O}$ as the point at ∞ or ~~zero~~ point

$\mathcal{O}$: Zero point / Point at ∞

This acts as Identity of '+' operator

i.e. $\boxed{P+\mathcal{O}=P}$

These are Same { Additive ~~Identity~~ ~~zero~~ point, Point at ∞

Thus E set of points over $E_p(a,b)$

Operator : + (as Defined earlier)

forms Abelian Group

Properties:

(1) Closure: It can be proven that adding 2 points (as defined earlier) can create another point on the curve.

(2) Associativity: $(P+Q)+R = P+(Q+R)$

(3) Commutative: $P+Q = Q+P \quad \forall P, Q \in E$

(4) Identity: O: Point at ∞ is the additive Identity

(5) Inverse: For every point P on the curve there exist a point Q such that

$$P+Q = O$$

i.e. If $P = (x_1, y_1)$

$Q = (x_1, -y_1)$ is such that $P+Q = O$ (See case (3) for operator '+')

→ We will accept the closure property

Note: $E_p(a,b)$ must be Non-singular i.e. $4a^3+27b^2 \neq 0$ (Why?)

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

↳ Non singular curve

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

$F(x,y): y^2 - x^3 - ax - b = 0$

Curve is singular at point (x_0, y_0) if

$$\frac{\partial F(x_0,y_0)}{\partial x} = \frac{\partial F(x_0,y_0)}{\partial y} = 0$$

$$\Rightarrow -3x_0^2 - a = 2y_0 = 0$$

$$\Rightarrow \boxed{y_0 = 0}, \quad \boxed{x_0^2 = \frac{-a}{3}}$$

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

$\therefore y_0^2 = x_0^3 + ax_0 + b \quad (\because (x_0, y_0) \in E_p(a,b))$

$\therefore 0 = x_0^3 + ax_0 + b$

$\therefore 0 = x_0^4 + ax_0^2 + bx_0$

$\therefore 0 = \frac{a^2}{9} + a\cdot\left(\frac{-a}{3}\right) + bx_0$

$\therefore 0 = \frac{a^2}{9} - \frac{3a^2}{9} + bx_0$

$\therefore \frac{2a^2}{9} = bx_0 \quad \therefore \boxed{x_0 = \frac{2a^2}{9b}}$

We know that, $3x_0^2 + a = 0$ $\left(\because -3x_0^2 - a = 0\right)$

$\therefore 3\left(\frac{4a^4}{81b^2}\right) + a = 0$

$\therefore \frac{4a^4}{27b^2} + a = 0$

$\therefore 4a^4 + 27ab^2 = 0$

$\therefore a(4a^3 + 27b^2) = 0$

$\therefore \boxed{4a^3 + 27b^2 = 0}$ if $a \neq 0$.

$\therefore$ If $4a^3 + 27b^2 = 0$ then Curve is singular at (x_0, y_0)

$\therefore$ It is important to have Non singularity condition i.e. $4a^3 + 27b^2 \neq 0$.