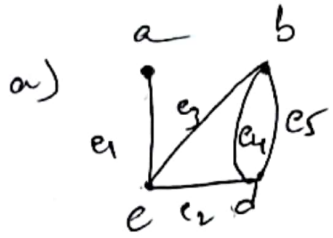
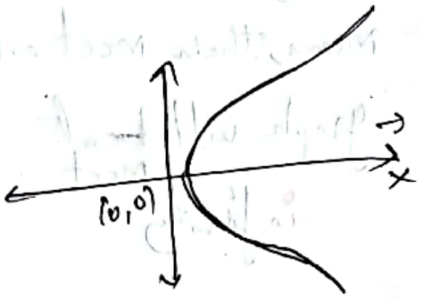
a) 

	e_1	e_2	e_3	e_4	e_5
a	1	0	0	0	0
b	0	0	1	1	1
c	1	1	0	0	0
d	0	1	0	1	1

⇒ Elliptic Curves :→

$(\mathbb{Z}_q, +) = \{[0], [1], [2], \ldots [6]\}$

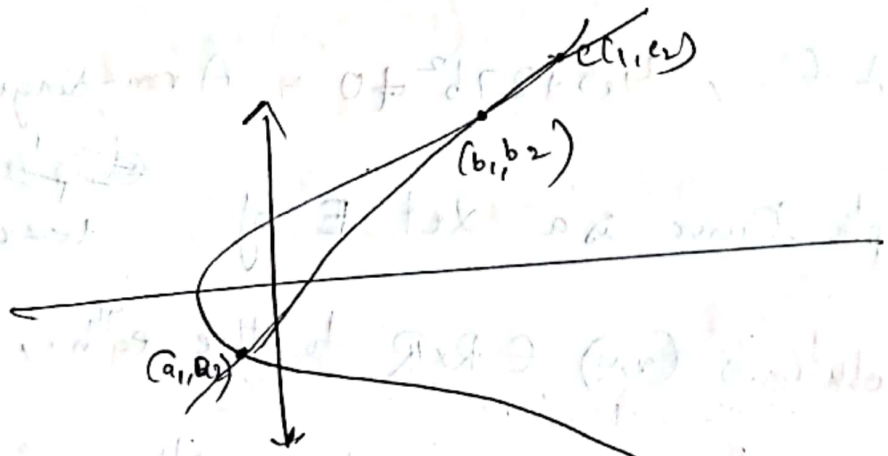
Primitive element → This can generate all other element on the given condition of operation.



→ This is symmetry over x^n.

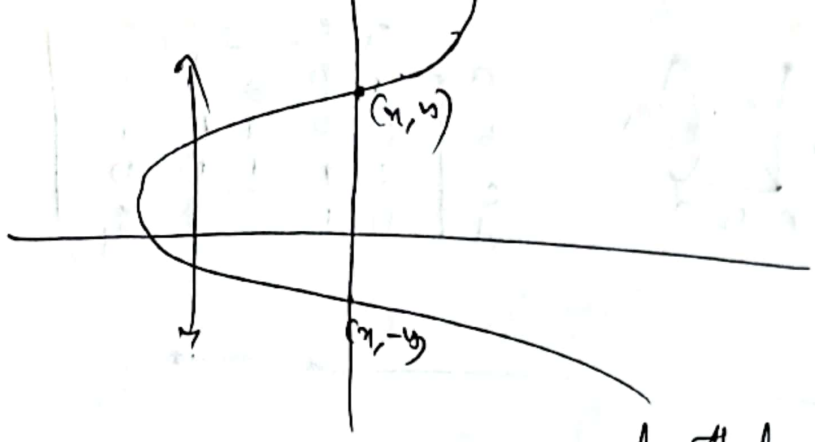
Elliptic Curve eq^{th} → $y^2 = x^3 + ax + b$ and

Condition → $4a^3 + 27b^2 \neq 0$.



we have to consider (a_1, a_2), (b_1, b_2) and write line eqth and find another point on graph (c_1, c_2)

Mental



This (x,y), $(x,-y)$ are two points that are

Consider then, It will never meet the graph

again. So, some x-coordinate will give "0"

$(x,y) + (x,-y) = 0$ → point of infinity

⇓

Means, their meet on graph will ~~leaf~~ meet in infinity

⇒ The line of single point can be told as "Tangent".

⇒ $a, b \in R$, $4a^3 + 27b^2 \neq 0$ ⇒ A non-singular ~~Elliptic~~ curve

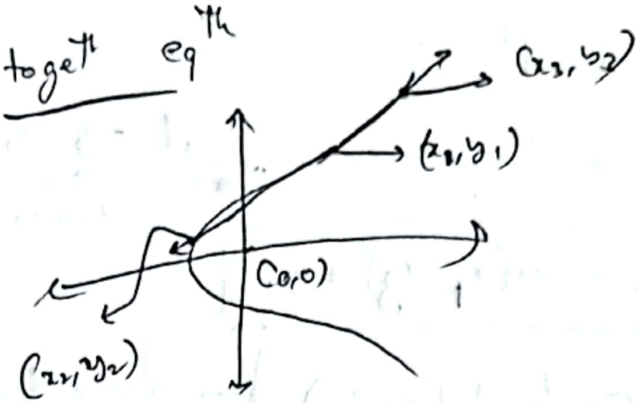
Eliptic Curve is a set E of

Solutions $(x,y) \in R \times R$ to the eqⁿ.,

$y^2 = x^3 + ax + b$, Together with a point "0",

a point at infinity.

⇒ How to get eq^{n}



⇒ $(y_2 - y_1) = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$ → Line eq^{n}

↳ $d = \frac{y_2 - y_1}{x_2 - x_1}$

Case 1 ⇒ $(x_1 \neq x_2)$

$y = dx + c$ → (1)

Substitute (x_1, y_1) in (1)

$c = y_1 - dx_2$ → (2)

from (1) & (2) ⇒ $\boxed{y = dx + (y_1 - dx_2)}$ → eq^{n}

The eq^{n} → $y^2 = x^3 + ax + b$ ← to get 3rd point

$$(dx + (y_1 - dx_2))^2 = x^3 + ax + b.$$

$$(dx)^2 + (y_1 - dx_2)^2 + 2dx(y_1 - dx_2) = x^3 + ax + b.$$

↳ from this, we get (x_1, x_2, x_3)

roots → $\{x_1, x_2, x_3\}$ → $y_3 = dx_3 + c$.

(we get y_3 from this)

$x_1 + x_2 + x_3 = d^2$

$x_3 = d^2 - x_2 - x_1$

$d = \frac{-y_3 - y_1}{x_3 - x_1}$

$\Rightarrow \boxed{y_3 = d(x_3 - x_3) - y_1}$

So, we can find (x_3, y_3) from above two eq^n.

Case 2 $\Rightarrow$ $x_1 = x_2$ and $y_1 = -y_2$

$(x_1, x_2) + (x_1, y_2) = O \leftrightarrow$ No intersection.

Case 3 $\Rightarrow$ (x_1, y_1) and Tangent 2 ecology.

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

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

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

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

$\Rightarrow$ Slope $\lambda = \frac{3x_1^2 + a}{2y_1}$

⇒ Number Theory →

(Continuation of Elliptic Curves)

$\mathbb{Z}_{11} = \{0, 1, \ldots, 10\}$

⇒ $y^2 = x^3 + x + 6$

$y(x)$

x	$f(x)$
0	6
1	8
2	
3	
4	
5	
6	
7	
8	
9	
10	

$y^2 \equiv 6 \pmod{11}$

$P \equiv 1 \bmod 4$

⇒ For $P > 3$, (Prime → P), the Elliptic Curve, $y^2 = x^3 + ax + b$, Over $\mathbb{Z}_p$ is the set of solns (x, y)

& solns $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence,

$y^2 \equiv x^3 + ax + b \pmod{p}$. $a, b \in \mathbb{Z}_p$ are constants such that $4a^3 + 27b^2 \not\equiv 0 \bmod p$,

Together with O, the point of Infinity.

⇒ 1) $y^2 = x^3 + x + 6 \pmod{11}$

$y^2 = ax^3 + x + b$; $a = 1, b = 6$

$4a^3 + 27b^2 = 4 + 27(6)^2 \pmod{11}$

$= 8 \pmod{11}$

$4a^3 + 6b^2 \neq 0 \pmod{11}$

$y^2 = x^3 + x + 6 \pmod{11}$

x	f(x)	QR	y
0	6	–	
1	8	–	
2	5	✓	(4, 7)
3	3	✓	(5, 6)
4	8	–	
5	4	✓	(2, 9)
6	8	–	
7	9	✓	(3, 8)
8	9	✓	(3, 8)
9	7	–	
10	4	✓	(2, 9)

$1^2 \equiv 1 \pmod{11}$

$2^2 \equiv 4 \pmod{11}$

$3^2 \equiv 9 \pmod{11}$

$4^2 \equiv 5 \pmod{11}$

$5^2 \equiv 3 \pmod{11}$

$6^2 \equiv 3 \pmod{11}$

$7^2 \equiv 5 \pmod{11}$

$8^2 \equiv 9 \pmod{11}$

$9^2 \equiv 4 \pmod{11}$

$10^2 \equiv 1 \pmod{11}$

$Q_R \equiv \{1, 3, 4, 5, 9\}$ ← (1, 10), (2, 9)

(5, 6) (4, 7) (3, 8)

(13 points)

So finally we will have (2, 4), (2, 7), (3, 5), (3, 6)

(5, 4), (5, 9), (7, 3), (7, 8), (8, 3), (8, 8)

(10, 2), (10, 9), O ← point at infinity

⇒ 2) (x_1, y_1), (x_2, y_2)

a) If $x_1 = x_2$, $y_1 \neq y_2$

Slope $\Rightarrow \lambda = \frac{y_2 - y_1}{x_2 - x_1} \Rightarrow (\lambda \to \infty)$

Slope → infinity

$(x_1, x_2) + (y_1, y_2) = 0.$

b) If $x_1 \neq x_2$, $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$

$\left(\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} \pmod p \right)$

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

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

c) $x_1 = x_2$, $y_1 = y_2$.

$\lambda = (3x_1^2 + a)(2y_1)^{-1} \pmod p$

$x_3 = (\lambda^2 - 2x_1) \pmod p.$

$y_3 = \left(\lambda(x_1 - x_3) + y_1\right) \bmod p$

(from previous question)

⇒ $(2,4) + (5,9)$

$p \to 11$

a)

$\lambda = (9-4) \times (5-2)^{-1} \pmod p$

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

$\lambda = (5)(3)^9 \pmod{11}$

$\lambda = (5)(4) \bmod 11$ ⇒ $\lambda \equiv 9 \bmod 11$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod 11$$

$$= (81 - 2 - 5) \bmod 11$$

$$x_3 = (8) \bmod 11$$

$$y_3 = \lambda(x_3 - x_1) + y_1 \pmod{11}$$

$$y_3 = 9(8 - 2) + 4 \pmod{11}$$

$$y_3 \equiv 3 \pmod{11}$$

$$(x_3, y_3) \equiv (8, 3)$$

ii) $(2,4) + (2,7)$

$$\lambda = 3/0 \Rightarrow (\lambda \to \infty)$$

So, point at infinity.

$$\therefore (2,4) + (2,7) = \mathcal{O}$$

iii) $(3,5) + (3,5)$

$$\lambda = (3x_1^2 + a)(2y_1)^{-1} \pmod{11}$$

$$\lambda = (3(3) + 1)(2 \times 5)^{-1} \pmod{11}$$

$$\lambda = (28)(10)^{-1} \pmod{11}$$

$$\lambda = (-6) \pmod{11} \equiv 5 \bmod 11)$$

$x_3 = d^2 - 2x_1 \pmod{11}$

$= 25 - 6 \pmod{11}$

$\equiv 19 \pmod{11} \equiv 8 \pmod{11}$

$y_3 = 5(5) + 5 \pmod{11}$

$= 30 \pmod{11}$

$\equiv 8 \pmod{11}$

$(x_3, y_3) \equiv (8, 8)$