Bitcoin:
Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010, Spring 2025

Dr. Christian Kümmerle

Lecture 10

Arithmetic on Elliptic Curves

UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

Main Reference:
- "Programming Bitcoin: Learn How to Program Bitcoin from Scratch", Jimmy Song, 1st Edition, O'Reilly, 2019, Chapters 2 and 3

Elliptic Curves

WHAT IS AN ELLIPTIC CURVE?

Set of solutions $S_{a,b} = \{(x,y) : y^2 = x^3 + a\cdot x + b\}$ for some a, b.

Used in Bitcoin (ECDSA):

$S_{0,7} = \{(x,y) : y^2 = x^3 + 7\}$ (choose $a = 0$, $b = 7$)

Name: "secp256k1"

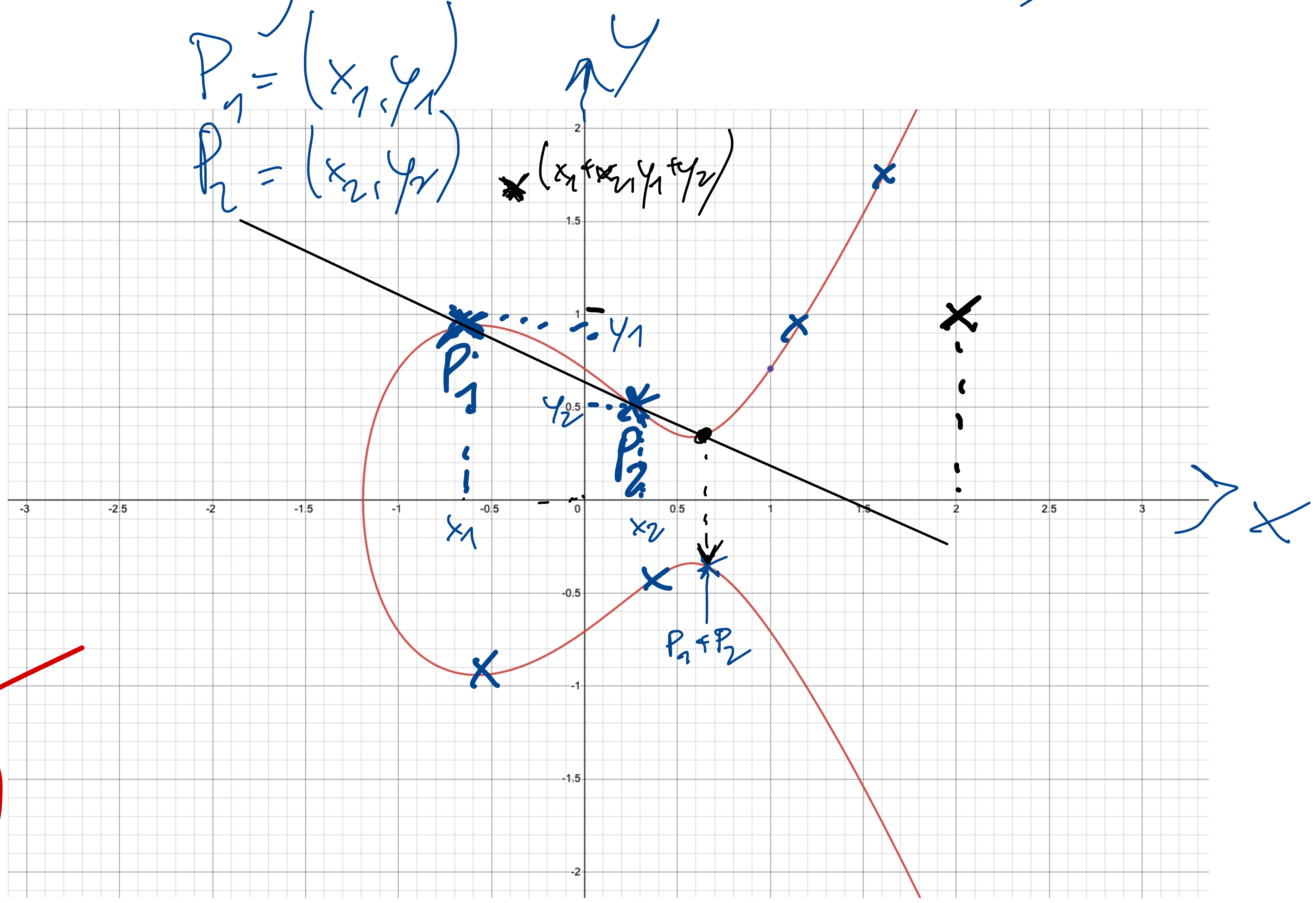
Q: Is $(x,y) = (2,1)$ a point on $S_{a,b}$?

LHS: $y^2 = 1^2 = 1$

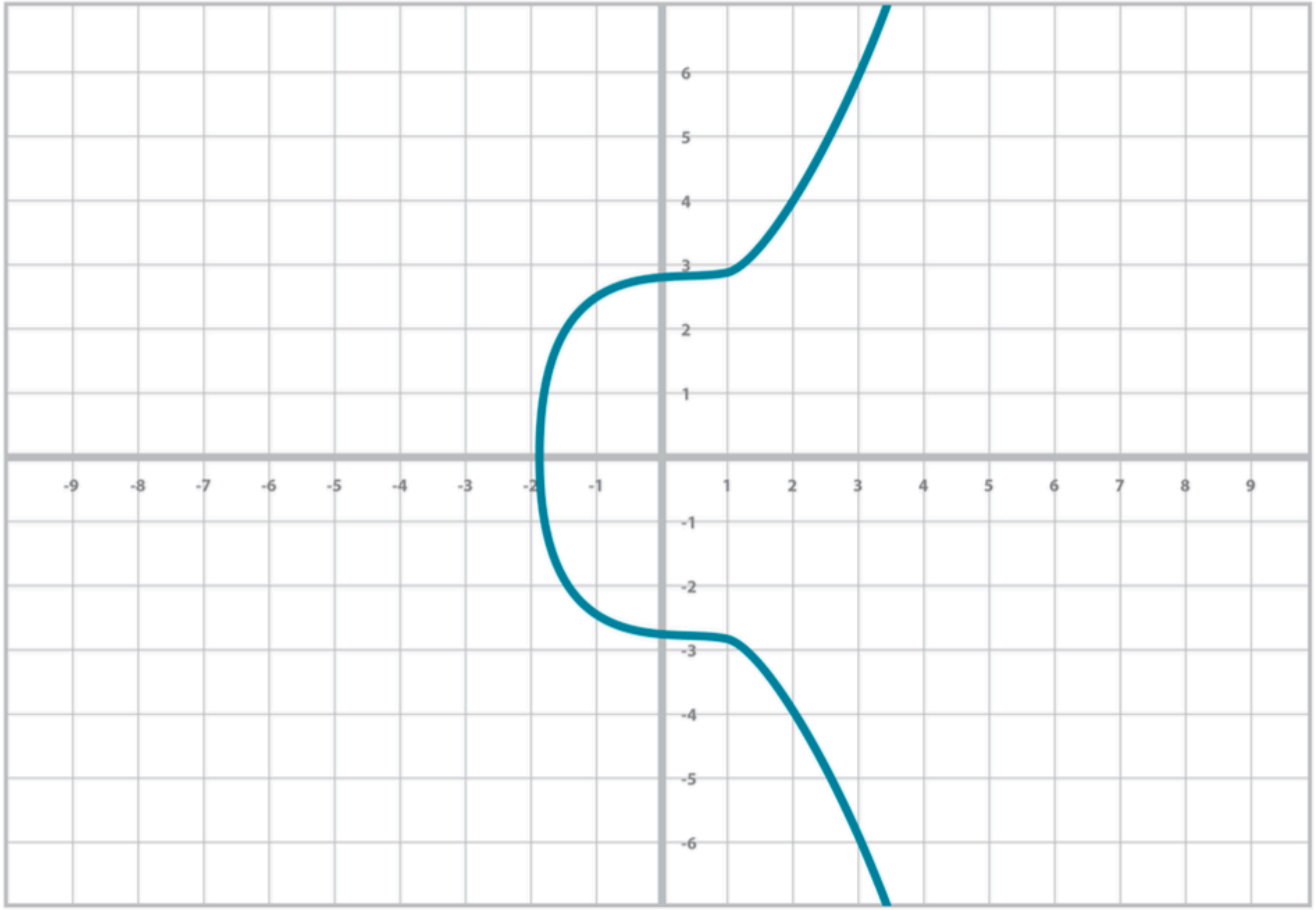
RHS: $x^3 + ax + b = 2^3 + a\cdot 2 + b$

$= 8 + 2a + b$

$a=0, b=7$: $= 15$



ELLIPTIC CURVE SECT256K1



EC equation:

$$y^2 = x^3 + 7$$

$S_{a,b} = \{(x, y) : y^2 = x^3 + ax + b\}$
with $a = 0$ and $b = 7$.

Goal: Define addition "+" of points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ for $P_1, P_2 \in S_{a,b}$ (points on the elliptic curve $S_{a,b}$)

We will use following fundamental result

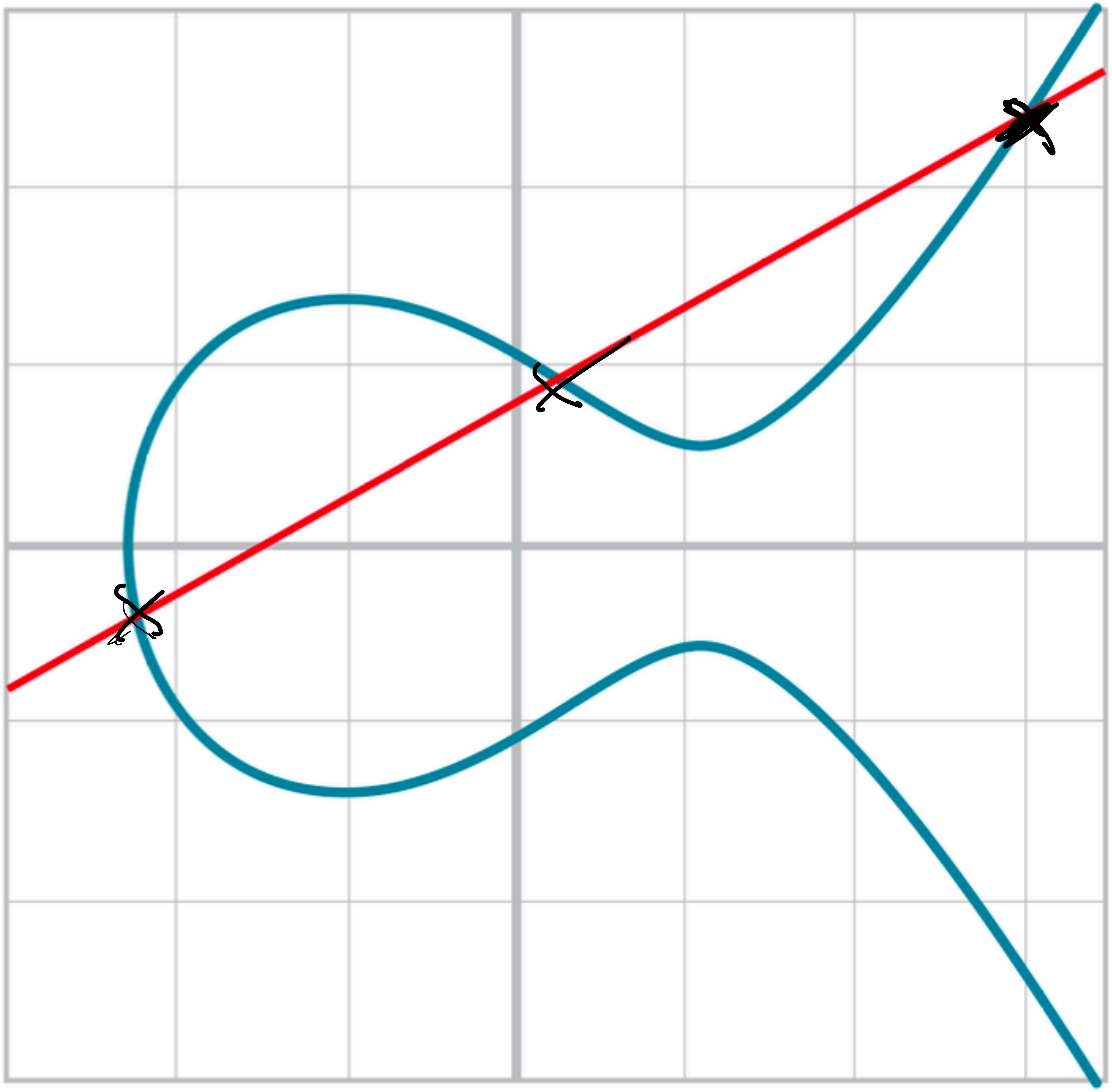
Theorem: (Special case of Bézout's thm.)

An elliptic curve intersects with a straight line either
(a) ▷ exactly at three points (counting tangential intersections twice)
(b) ▷ exactly once, or
(c) ▷ exactly twice (in which case line is vertical)

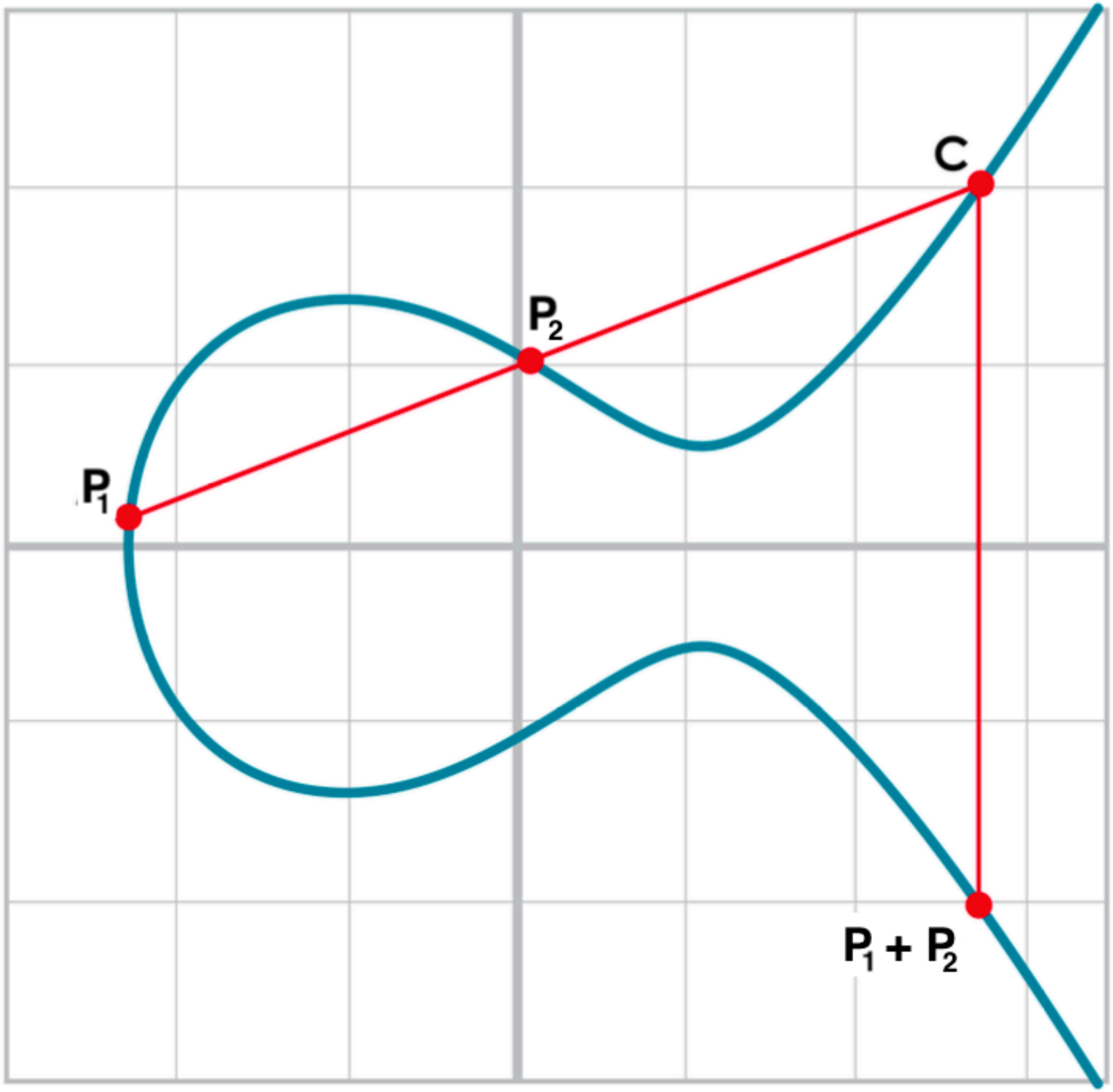
LINES AND ELLIPTIC CURVES: CASE OF LINE INTERSECTING AT THREE POINTS

Case (a)

(Not tangential point)

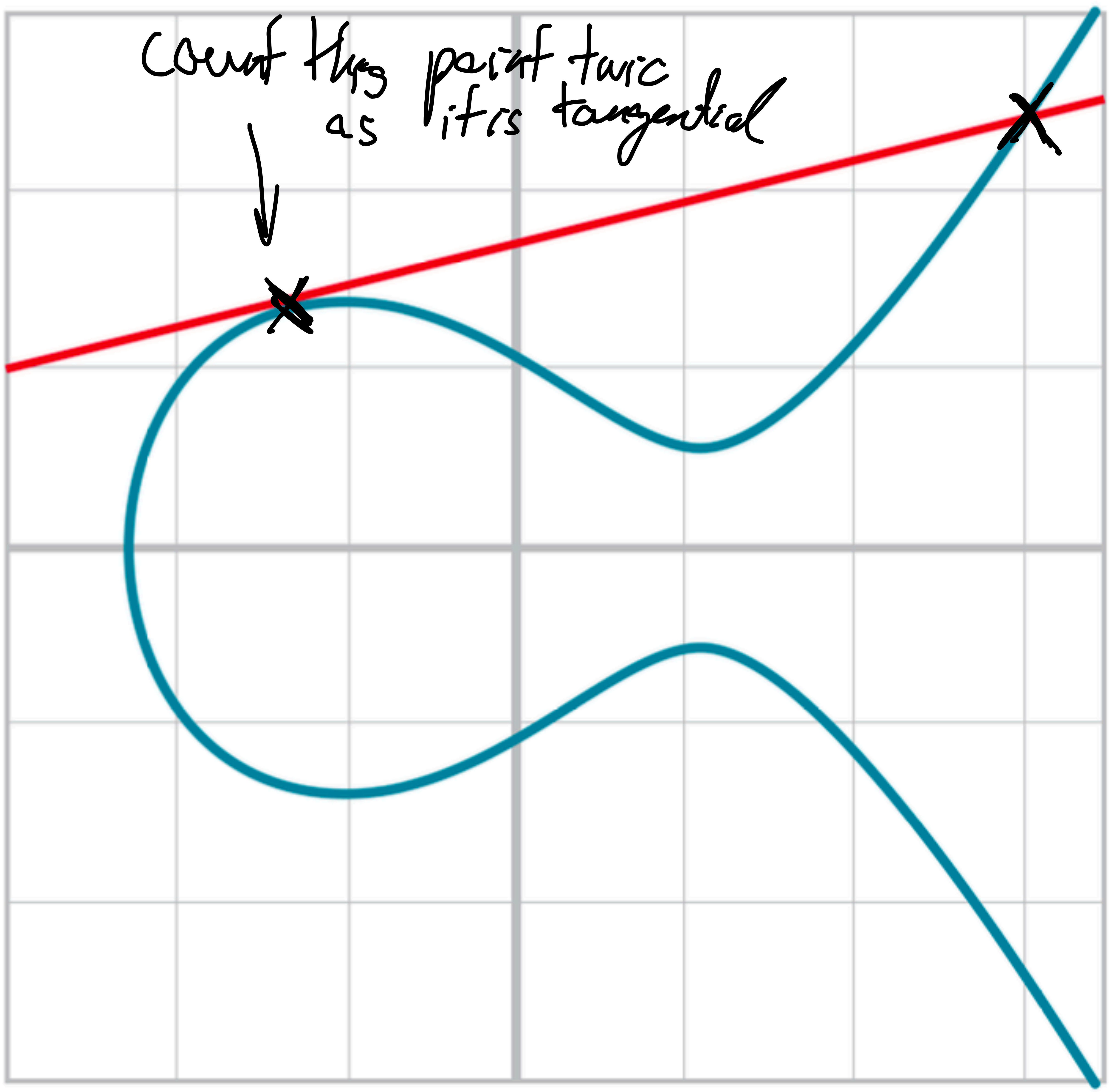


POINT ADDITION ON ELLIPTIC CURVES



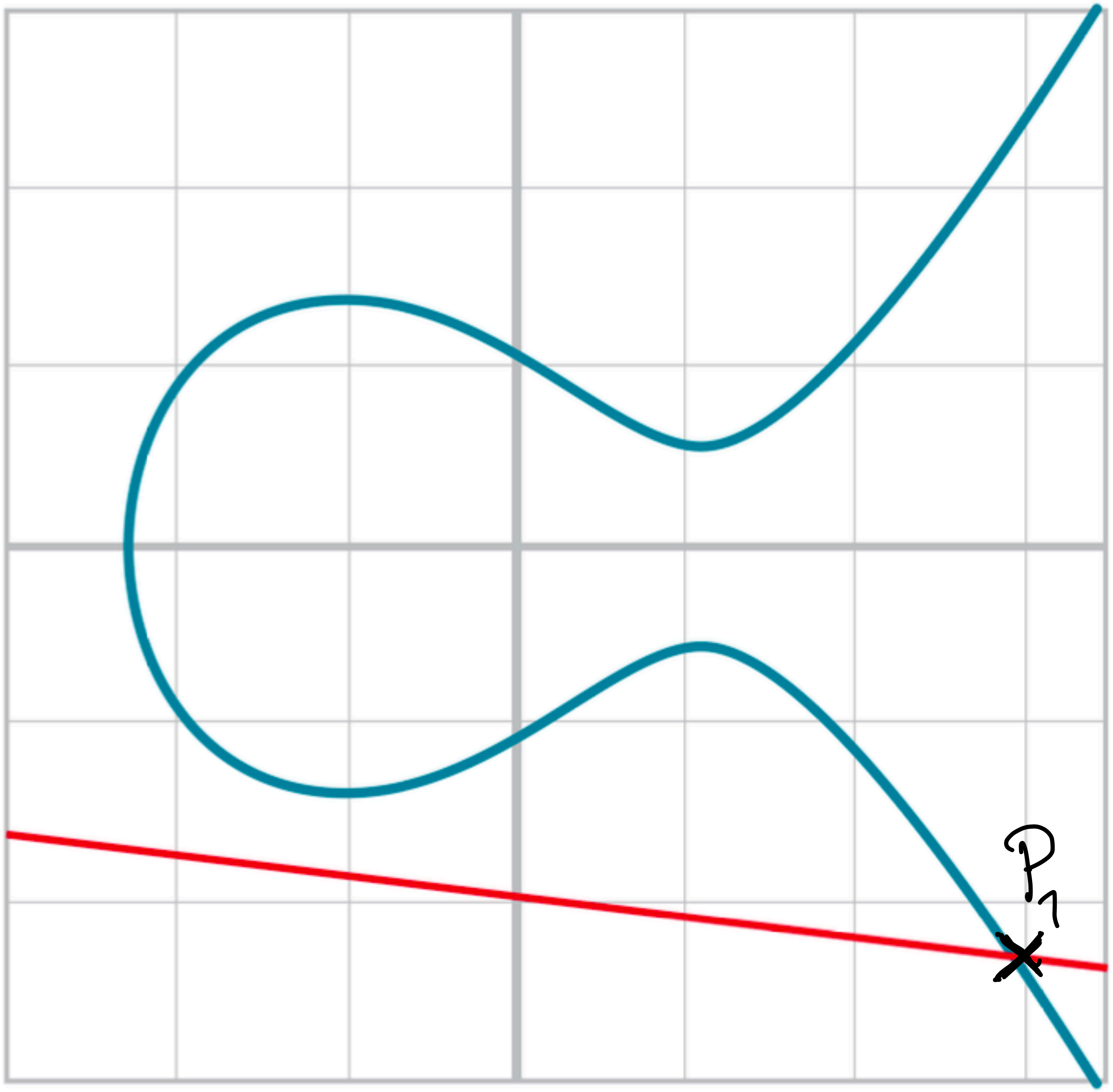
LINES AND ELLIPTIC CURVES: INTERSECTING AT ONE POINT AND ONE TANGENTIAL POINT

Case (a)

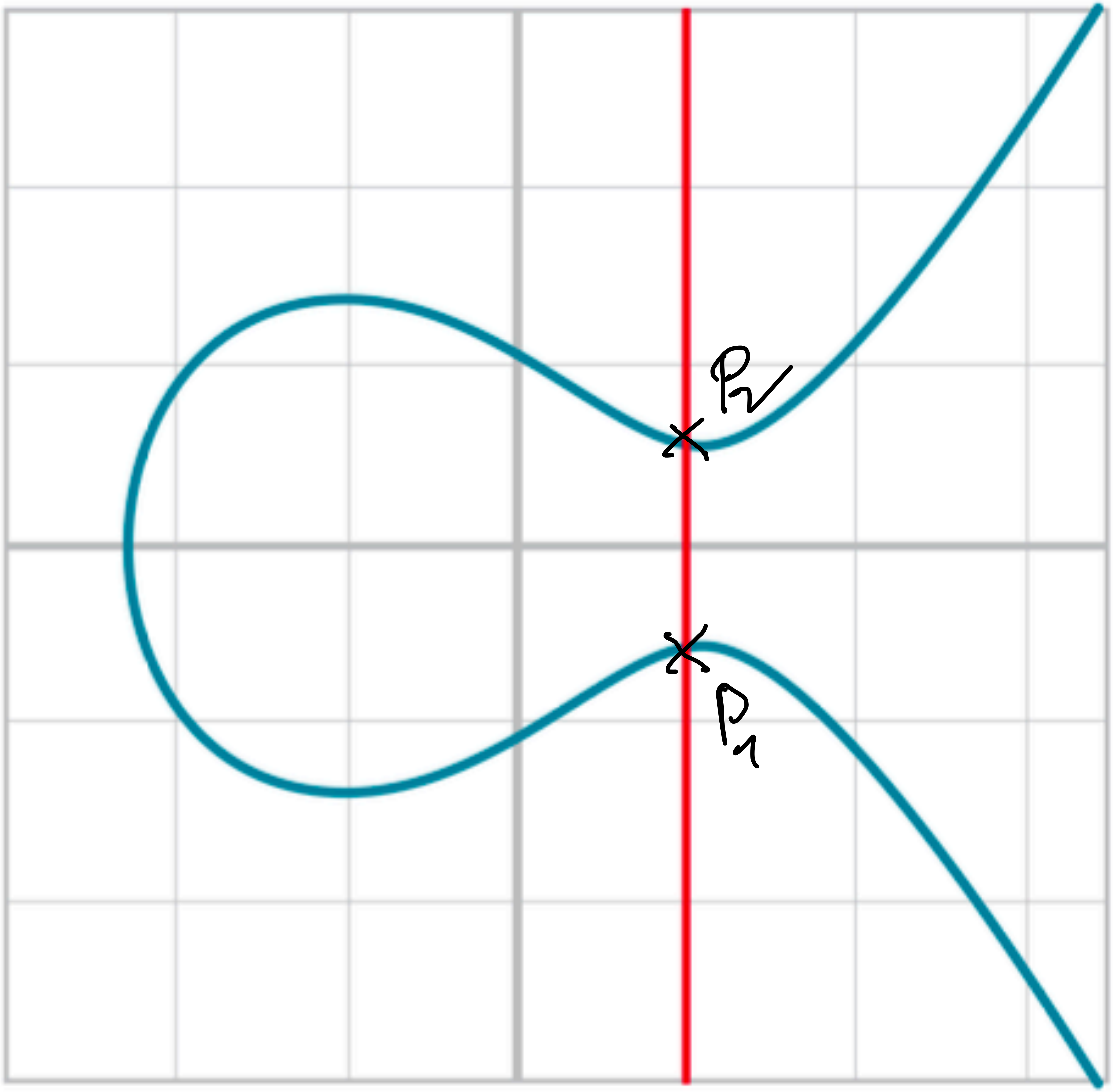


LINES AND ELLIPTIC CURVES: CASE OF LINE INTERSECTING AT ONLY ONE POINT

Case: (b)



CASE (C): TWO POINTS, CONNECTED BY VERTICAL LINE

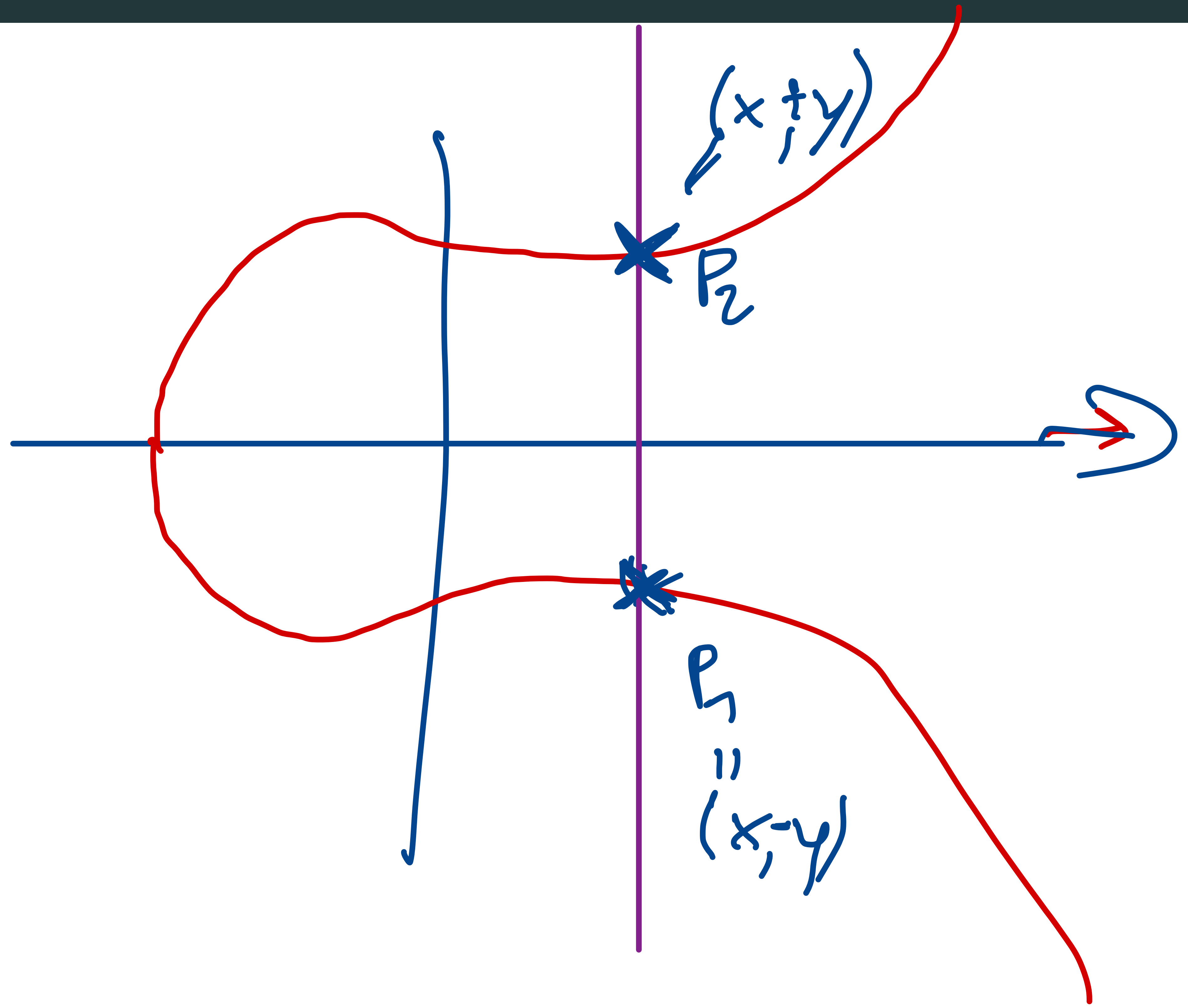


Case (c): We define: $P_1 + P_2 = \mathcal{O}$

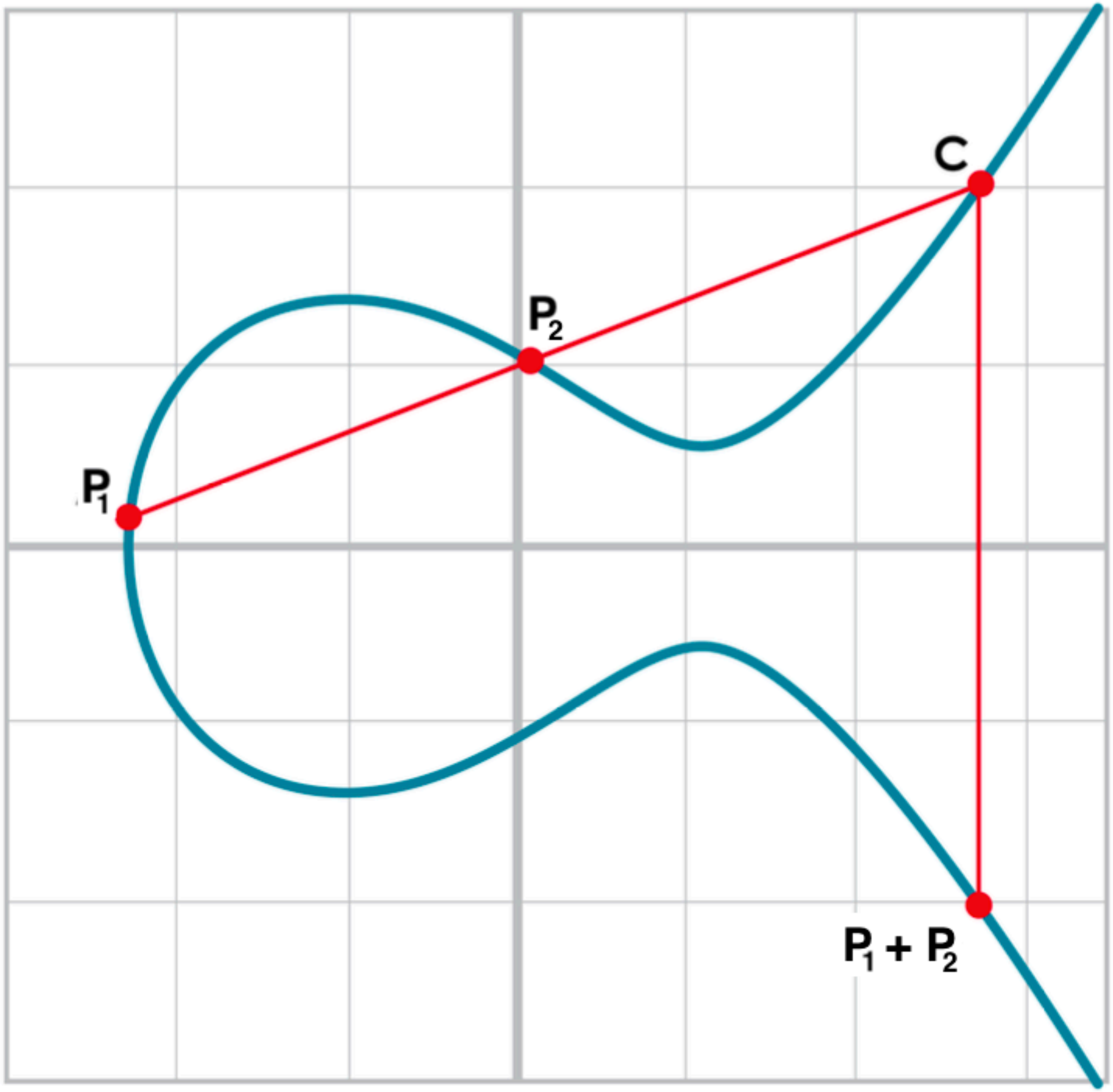
"$\mathcal{O}$" is "point at infinity"

$\Rightarrow$ P_2 is additive inverse of P_1

$\hookrightarrow$ $P_2 = -P_1$



POINT ADDITION ON ELLIPTIC CURVES



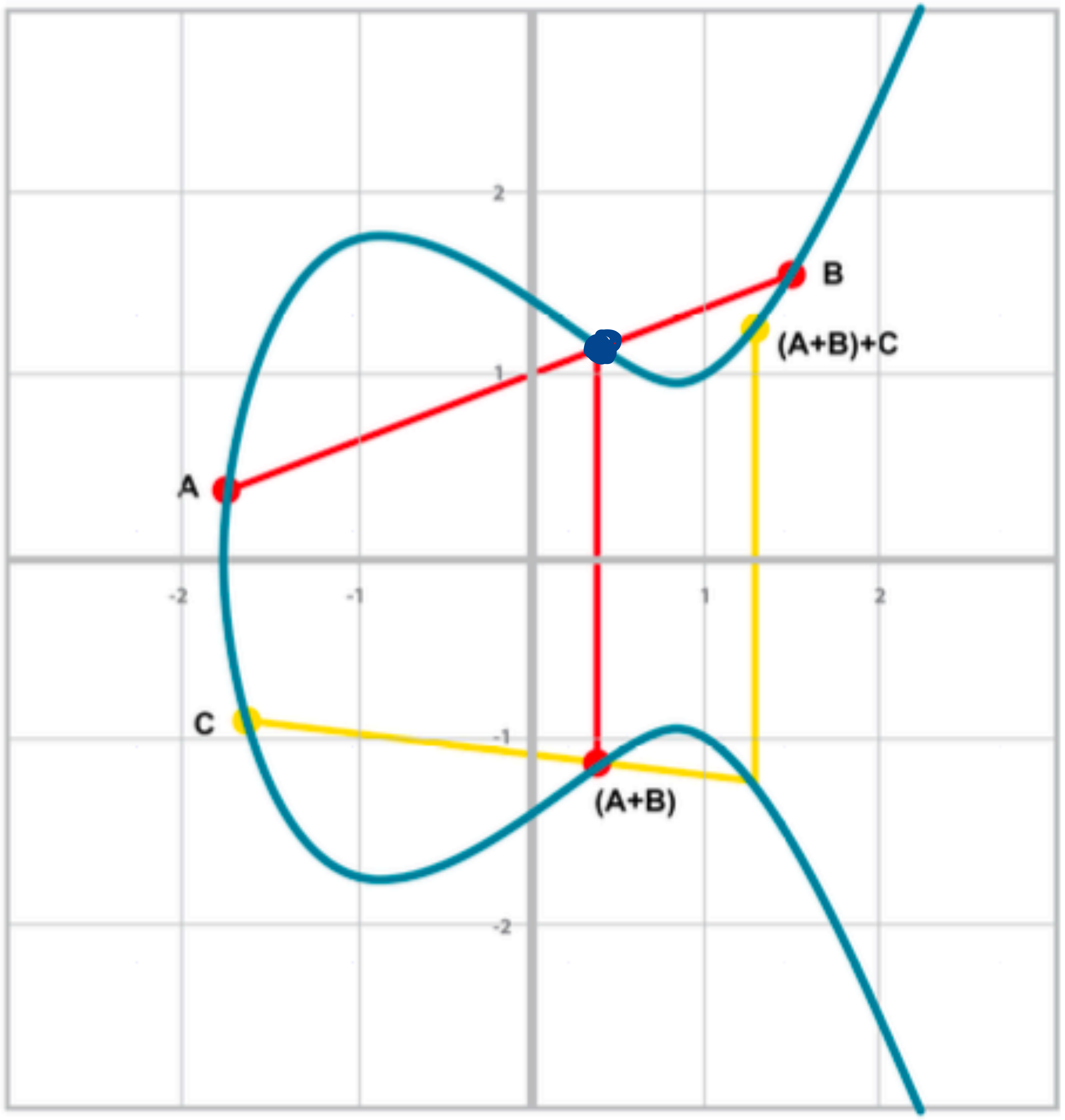
Q: Why do we need to "reflect" C at x-axis to define $P_1 + P_2$?

Answer:

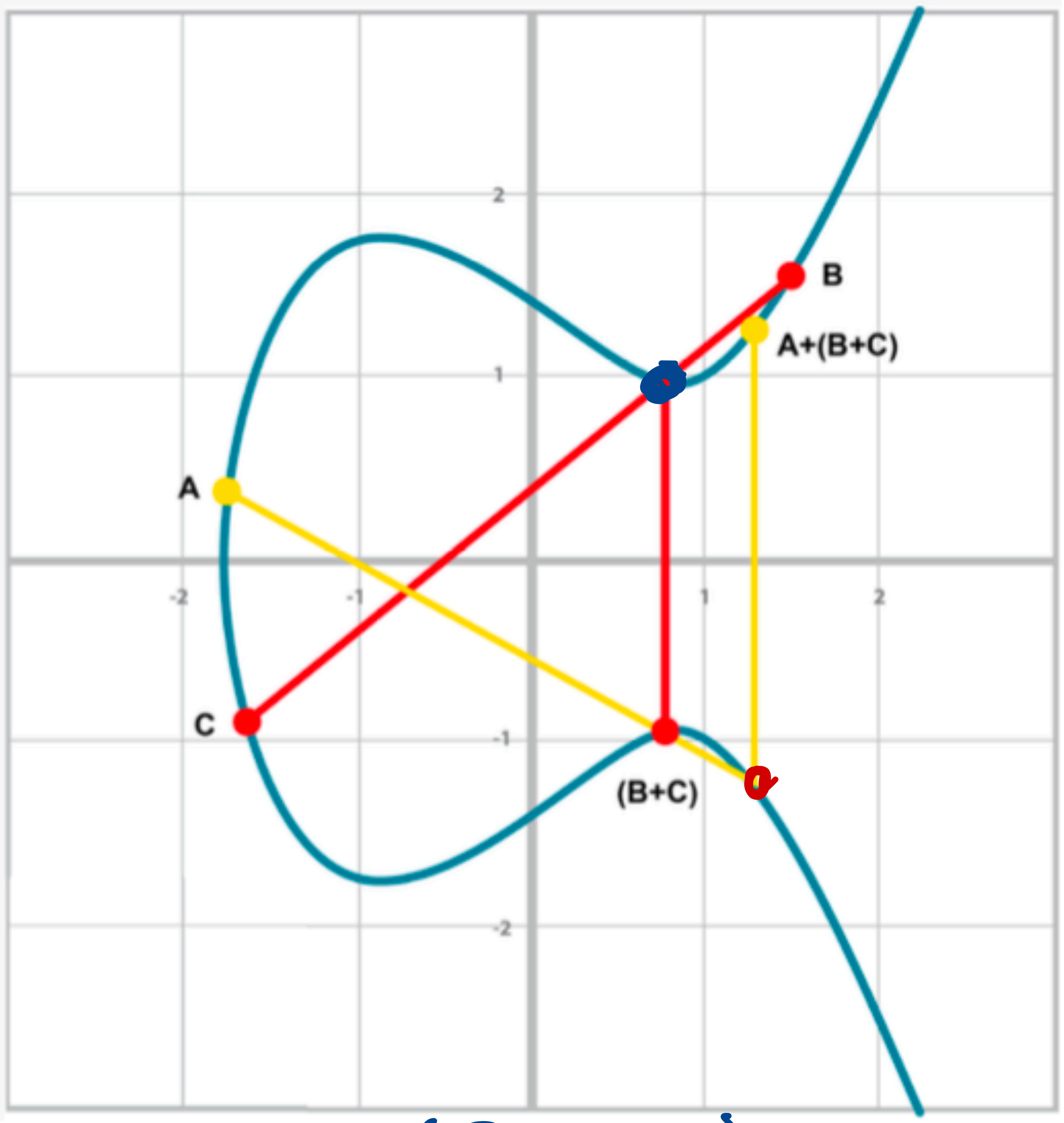
We need associativity.

POINT ADDITION ON ELLIPTIC CURVES

We need: $(A+B)+C = A+(B+C)$



$(A+B)+C$



$A+(B+C)$

POINT ADDITION ON ELLIPTIC CURVES

If $A = (x_1, y_1) \in S_{a,b}$, $B = (x_2, y_2) \in S_{a,b}$ are two points on elliptic curve $S_{a,b} := \{(x,y) : y^2 = x^3 + ax + b\}$, the desirable properties of point addition:

(i) $(A+B)+C = A+(B+C)$ "associativity"

(ii) $A + B = B + A$ "commutativity"

(iii) $A + \mathcal{O} = A$ for "point at infinity" $\mathcal{O}$ "additive identity"

(iv) There exists an additive inverse $-A$ s.t. $A+(-A) = \mathcal{O}$ for all $A \in S_{a,b}$.

$$\boxed{\begin{aligned} 2A &:= A+A \\ 3A &= A+A+A \\ &\dots \end{aligned}}$$

POINT ADDITION ON ELLIPTIC CURVES

$A = (x_1, y_1) \in S_{a,b}$, $B = (x_2, y_2) \in S_{a,b}$

Case 1: $x_1 \neq x_2$

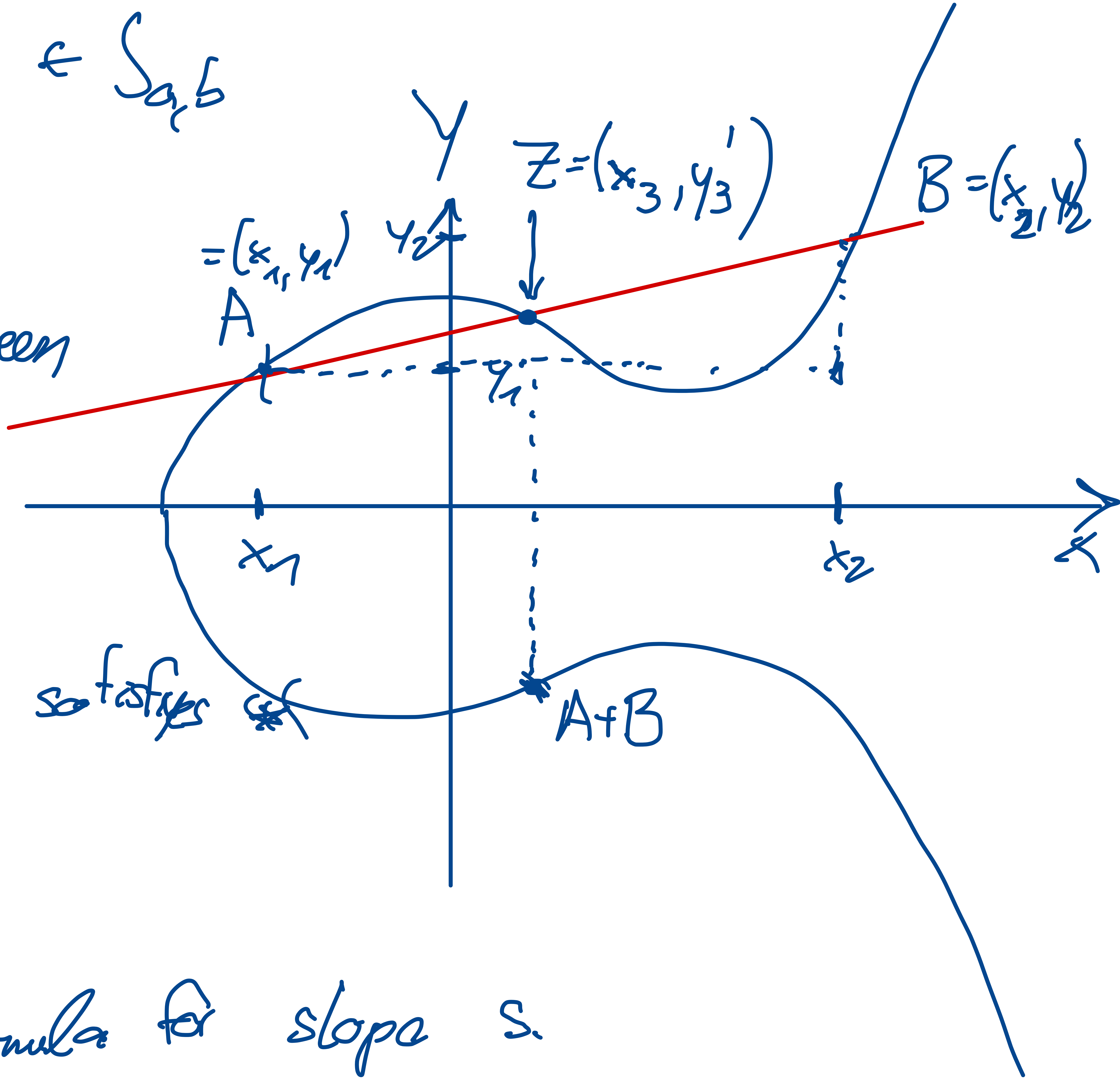
Idea: Define line equation of line between A and B:

$$\boxed{y = s(x - x_1) + y_1} \quad (*)$$

- We observe: Inserting $x = x_1$ and $y = y_1$ satisfies $(*)$
- Insert $x = x_2$, $y = y_2$:

$$y_2 = s(x_2 - x_1) + y_1$$

$$\Rightarrow \quad s = \frac{y_2 - y_1}{x_2 - x_1} \quad \Rightarrow \text{Formula for slope } s.$$



POINT ADDITION ON ELLIPTIC CURVES

To find point Z, we need:

(I) $\boxed{y = s(x-x_1)+y_1}$ line equation with $s = \frac{y_2-y_1}{x_2-x_1}$

(II) $y^2 = x^3 + ax + b$ (elliptic curve equation)

$(a+b)^2 = a^2 + 2ab + b^2$

Squaring (I) and plugging into (II):

$$[s(x-x_1)+y_1]^2 = x^3 + ax + b$$

$$\Leftrightarrow s^2(x-x_1)^2 + 2\cdot s(x-x_1)y_1 + y_1^2 = x^3 + ax + b$$

$$\Leftrightarrow x^3 - (s^2x^2 - 2s^2x_1x + s^2x_1^2) - 2sxy_1 + 2sx_1y_1 + ax + b - y_1^2 = 0 \quad (**)$$

We know: x_3 (first coordinate of Z) needs to satisfy (**)

$$\Rightarrow \underbrace{x^3-(s^2x^2-2s^2x_1x+s^2x_1^2)-2sxy_1+2sx_1y_1+ax+b-y_1^2}_{=(f)}$$

$$= (x-x_1)\cdot(x-x_2)\cdot(x-x_3)$$

since $x=x_1$ and $x=x_2$ are the two other solutions of (**)

$$(f) = (x^2-x_1x-x_2x+x_1x_2)(x-x_3) =$$

$$= x^3-x_1x^2-x_2x^2+x_1x_2x-x_3x^2+x_1x_3x+x_2x_3x-x_1x_2x_3$$

$$= x^3+(-x_1-x_2-x_3)\,x^2+\dots\dots$$

We can now match 2nd order coefficients of equation (the ones infront of x^2).

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

POINT ADDITION ON ELLIPTIC CURVES

$\Rightarrow$ We can compute x_3 given

- x_1 (first coordinate of A)
- x_2 (first coordinate of B)
- s (defined as $s = \frac{y_2 - y_1}{x_2 - x_1}$).

y-coordinate y_3' of Z:

From line equation $y_3' = s(x_3 - x_1) + y_1$

We obtain $A + B = (x_3, y_3)$ by setting

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

Summary:

1) $s = \frac{y_2 - y_1}{x_2 - x_1}$
2) $x_3 = s^2 - x_1 - x_2$
3) $y_3 = s(x_1 - x_3) - y_1$

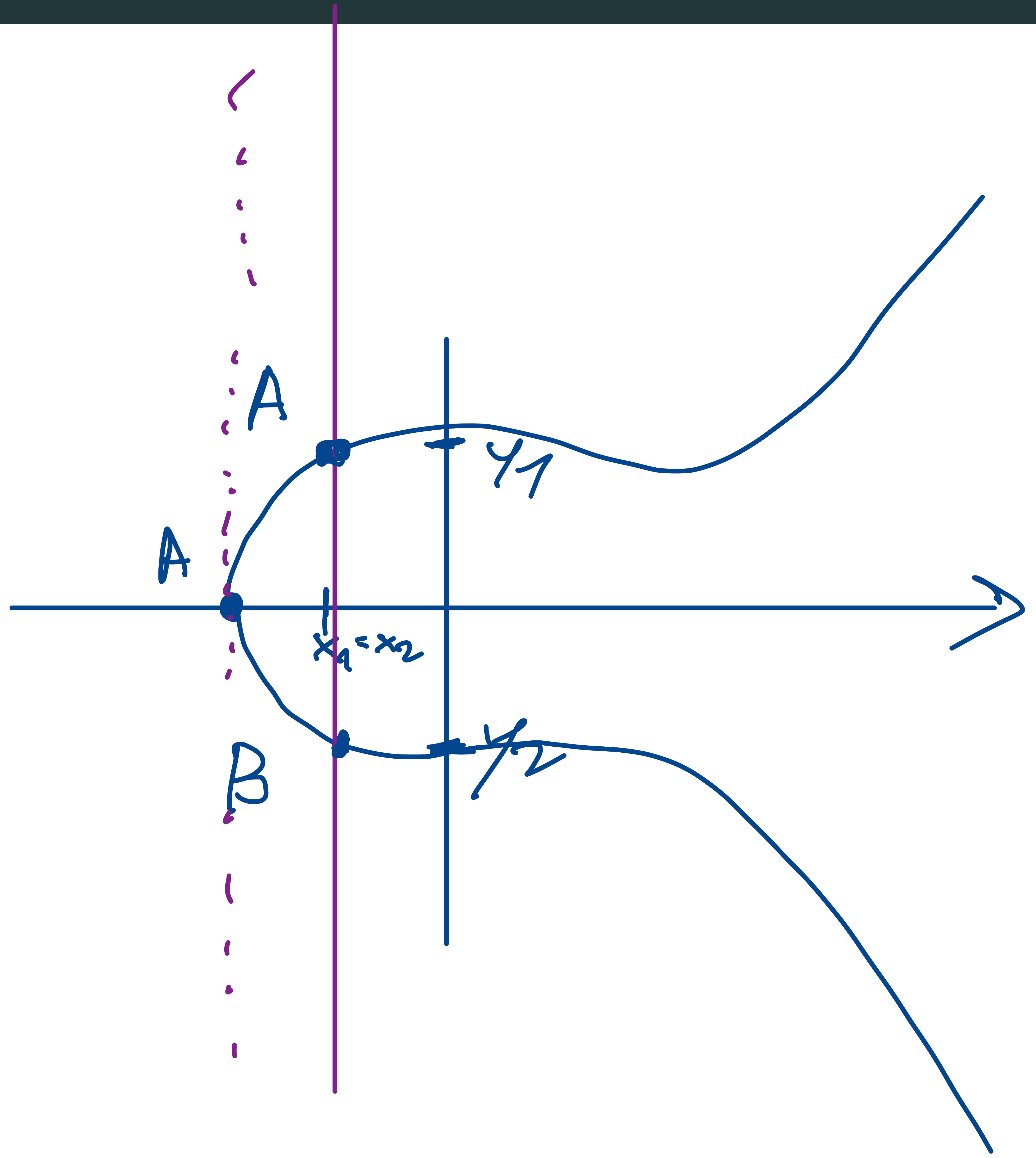
POINT ADDITION ON ELLIPTIC CURVES

$A = (x_1, y_1) \in S_{a,b}$, $B = (x_2, y_2) \in S_{a,b}$

Case 2: $x_1 = x_2$, and $y_2 = -y_1$

$\Rightarrow$ Case of straight line being vertical

$P := A + B = \mathcal{O}$, point at infinity



$A = (x_1, y_1) \in S_{a,b}$, $B = (x_2, y_2) \in S_{a,b}$

Case 3: $x_1 = x_2$, $y_2 = y_1$, $y_1 \neq 0$

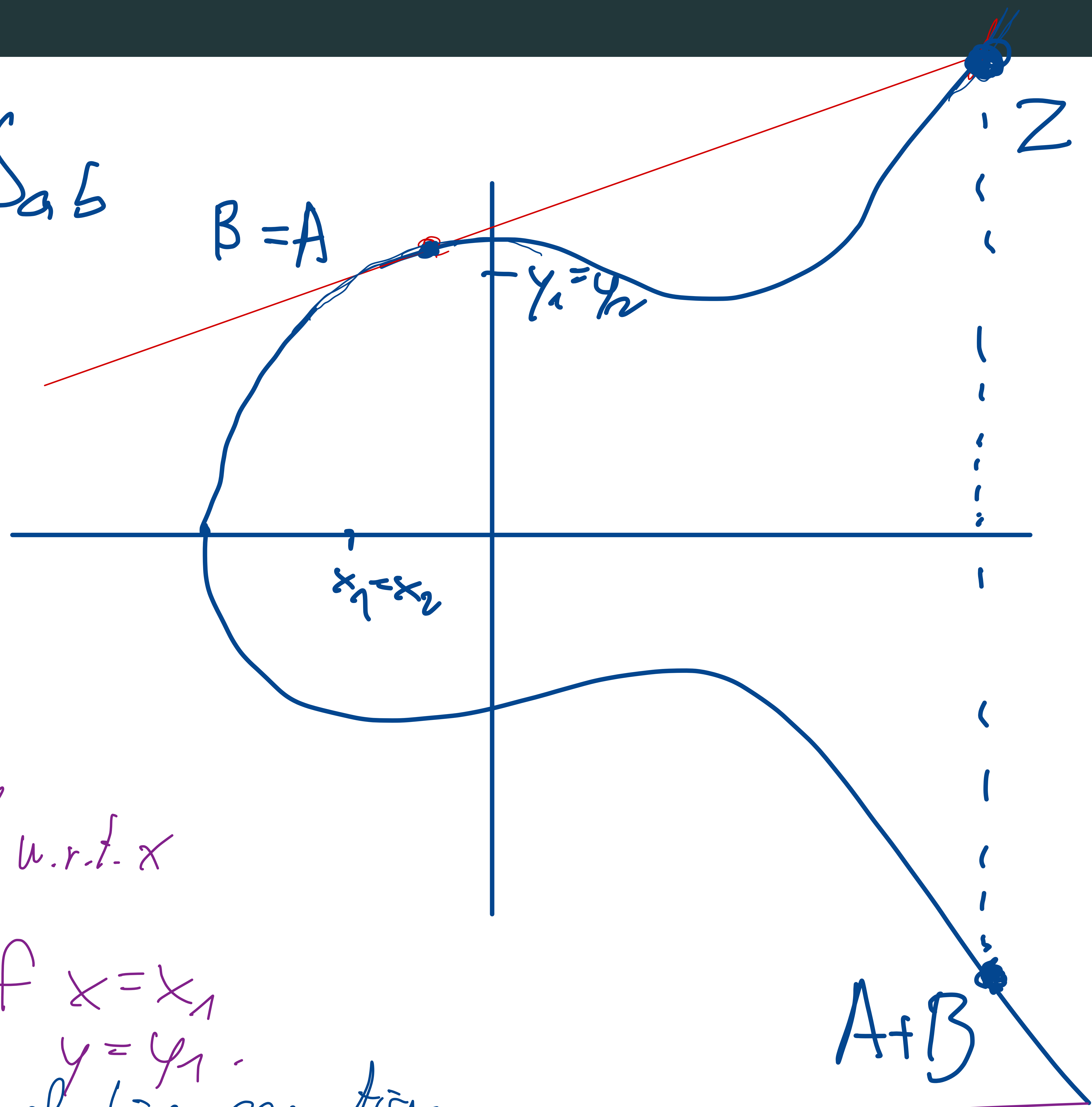
Idea: Consider $y^2(x) = x^3 + ax + b$

Take derivative $\Longrightarrow$ w.r.t. x on both sides

$$2y \cdot y' = 3x^2 + a + 0$$

derivative of $y = \sqrt{x^3 + ax + b}$ w.r.t. x

this is exactly slope s if $x = x_1$, $y = y_1$.



$$\Rightarrow \quad 2y_1 \cdot s = 3x_1^2 + a$$

$$\Longleftrightarrow \quad \boxed{s = \frac{3x_1^2 + a}{2y_1}}$$

slope s of line equation

$$y = s(x - x_1) + y_1$$

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

POINT ADDITION ON ELLIPTIC CURVES

Summary of steps to compute:

1) $$s = \frac{3x_1^2 + a}{2y_1}$$

As in case 1

2) $$x_3 = \left(s^2 - x_1 - x_2\right) \overset{x_2 = x_1}{=} s^2 - 2x_1$$

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

We want to define "multiples" of elliptic curve points.

E.g. Given $A=(x_1,y_1) \in S_{a,b}$, compute $3 \cdot A \in S_{a,b}$

⚠ Different from defining $A \cdot B$, where $A, B \in S_{a,b}$.

Define: $k \cdot A = \underbrace{A + A + \dots + A}_{k \text{ times}}$ if k is pos. integer

<u>Observation:</u> If we consider $S_{a,b}^{\mathbb{F}_p} = \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax + b\}$,

finite field of order p

then solving $k \cdot A = B$ for k (given $A, B \in S_{a,b}^{\mathbb{F}_p}$) is <u>extremely hard</u> if order p is very large.

SCALAR MULTIPLICATION ON ELLIPTIC CURVES

"discrete logarithm problem for elliptic curves"