Bitcoin:
Programming the Future of Money

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

Dr. Christian Kümmerle

Lecture 9

Finite Fields (part 2) & Elliptic Curves

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

Finite Fields

MOTIVATION TO STUDY FINITE FIELDS & ELLIPTIC CURVES

Indispensable to understand:

- **Elliptic Curve Digital Signature Algorithm (ECDSA)**
  - Fundamental cryptographic tool to “sign” transactions and spend bitcoin
  - Proposed by Neal Koblitz and Victor S. Miller in 1985, standardized in 2000
  - Main signature scheme used in Bitcoin

- **Schnorr Signatures on Elliptic Curves**
  - Proposed by Claus-Peter Schnorr in 1990, but patented and not freely available until 2010
  - Implemented in address format introduced by 2021 Taproot upgrade

FINITE FIELDS

Def: A field $(F, +, \cdot)$ is a set F that together with two operations "$+$" (called addition) and "$\cdot$" (called multiplication) satisfy the following properties:

1) If $a, b \in F$, then $a+b \in F$, $a \cdot b \in F$ ("closedness")
2) A element $0 \in F$ called additive identity exists and satisfies $a+0=a$ for any $a \in F$
3) An element $1 \in F$ called multiplicative identity exists and satisfies $a \cdot 1 = a$ for any $a \in F$.
4) For any element $a \in F$, there exists $-a \in F$ (additive inverse) $a+(-a)=0$
5) For any element $a \in F \setminus \{0\}$, there exists an element $a^{-1} \in F$ called multiplicative inverse with $a \cdot a^{-1} = 1$

EXAMPLES OF INFINITE & FINITE FIELDS

1) $\mathbb{R}$: real numbers → infinite field

-5.4 additive inverse

$5.4 \Rightarrow \frac{1}{5.4}$ multiplicative inverse etc.

2) Not a field: $\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$.

⚠: No additive inverse

3) Not a field: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

⚠ No multiplicative inverse: E.g., $-3 \cdot \left(-\frac{1}{3}\right) = 1$

4) Field (infinite): $\mathbb{Q}$: set of rational numbers

5) Finite field: $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ with appropriate notion of "+" and "·"

ORDER OF A FINITE FIELD

Def: The **order** of a field $(F, +, \cdot)$ is the number $|F|$ of elements in F

E.g.: If $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$, then $|F_2| = 7$

Observation: For any prime number p, we can define a finite field $F_p = \{0, 1, 2, \ldots, p-1\}$.

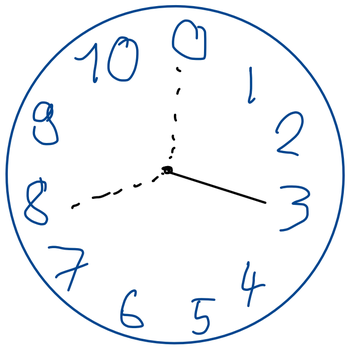
To make this work: "Redefine" "+" and "$\cdot$".

ADDITION WITHIN FINITE FIELDS

Let $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ be finite field, where p prime.

For $a, b \in \mathbb{F}_p$ we define the addition "+" such that

$$a + b := a \overset{+}{_p} b := (a+b) \,\%\, p$$



E.g.: ▷ $a = 3, \; b = 5, \; p = 11$: $\quad a + b = (3+5) \,\%\, 11 = 8 \,\%\, 11 = 8$

▷ $a = 3, \; b = 10, \; p = 11$: $\quad a + b = (3+10) \,\%\, 11 = 13 \,\%\, 11 = 2$

ADDITION WITHIN FINITE FIELDS

Accordingly, we can define subtraction within finite fields:

For any $a, b \in \mathbb{F}_p$: $a -_f b := a +_f (-b)_f := [a + (p - b)] \,\%\, p$.

(*)

"mod / modulo"

MULTIPLICATION WITHIN FINITE FIELDS

We need:

1) $a +_f b \in F_p$ if $a, b \in F_p$
2) For all $a \in F_p$, exists $1 \in F_p$ s.t. $a \cdot_f 1 = a$
3) For all $a \in F_p$, exists $a^{-1} \in F_p$ s.t. $a \cdot_f a^{-1} = 1$

↑ for this to hold, we need p prime (or order $= p^n$ with n integer)

We define multiplication within a finite field:

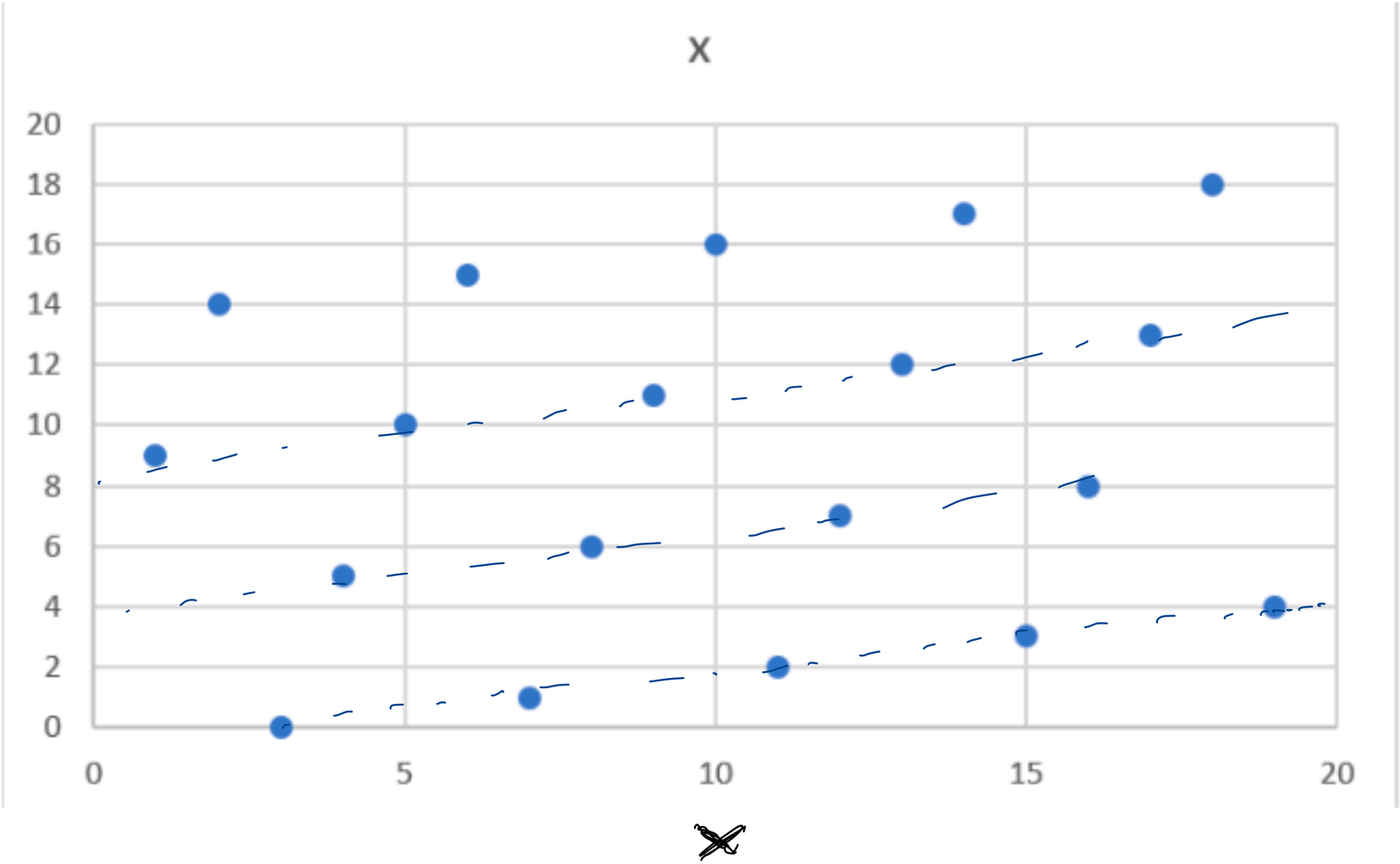
For any $a, b \in F_p$,

$$a \cdot_f b := \underbrace{a +_f a +_f \dots +_f a}_{\text{as integer} \rightarrow b \text{ times}}$$

Examples: 1) $a = 5$, $b = 3$, $p = 11$

$$5 \cdot_f 3 = (5 +_f 5) +_f 5 = [(5+5)\,\%\,11] +_f 5 = 10 +_f 5 = (10+5)\,\%\,11$$
$$= 15\,\%\,11 = 4$$

A LINE WITHIN A FINITE FIELD



Example: y = (x-3)/4 within F_{19}

EXAMPLE: MULTIPLICATION IN FINITE FIELDS

In F_{97}: $(p = 97)$

$$95 \cdot_f 45 \cdot_f 31 = ([95 \cdot 45] \% 97) \cdot_f 31$$

$$= ([-2 \cdot 45] \% 97) \cdot_f 31$$

$$= ([-90] \% 97) \cdot_f 31$$

$$= (7 \% 97) \cdot_f 31 \qquad = 23$$

$$= (2 \cdot 3 \cdot 31 + 31) \% 97 \qquad = 23 \% 97$$

$$= (2 \cdot 93 + 31) \% 97$$

$$= (2 \cdot (-4)) \% 97 + 31 \qquad = (31 - 8) \% 97$$

$$= (7 \cdot 31 \% 97)$$

EXPONENTIATION WITHIN FINITE FIELDS

If $a, b \in F_p$, we can define $a^b = (a \cdot_f a) \cdot_f \cdots \cdot_f a$ (b times)

$\cdot_f$: finite field multiplication

Motivation: If $3 \in \mathbb{R}$:

$3^2 = 3 \cdot 3 = 9 \in \mathbb{R}$

Eg: $a = 7, b = 3, p = 19$:

$7^3 = (7 \cdot_f 7) \cdot_f 7$

$= [(7 \cdot 7) \% 19] \cdot_f 7$

$= [49 \% 19] \cdot_f 7 = 11 \cdot_f 7$

$(2 \cdot 19 + 11) \% 19$

$= 77 \% 19$

$= (4 \cdot 19 + 1) \% 19$

$= 1$

$7^3 = 7 \cdot_f 7^2 = 1 \Rightarrow 7^{-1} = 7^2$

We observe 7^2 is multiplicative inverse of 7

FERMAT'S LITTLE THEOREM

Claim: $\{k \cdot n \; ; \; 1 \le n \le p-1\} = \{n : 1 \le n \le p-1\}$ for any $k \le p$ if p is prime

Q: How do we calculate $a^{-1} \in F_p$ for any $a \in F_p$?

$a^{-1} = 1/_{\mathbb{R}} a$

↑ used to define division

For "usual" division in $\mathbb{R}$:

- $7 \cdot 8 = 56 \Rightarrow 8 = 56/7$
- $12 \cdot 2 = 24 \Rightarrow 2 = 24/12$

Q: What is $7/_{\mathbb{R}} 5$?

$F_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

FERMAT'S LITTLE THEOREM

Theorem: If k is not divisible by p and if p is prime, then $k^{p-1} \% p = 1$

Proof: Let p prime. Multiply integers of set from claim on last slide with each other:

$$\{(k)\cdot(2k)\cdot(3k)\cdot\ldots(p-1)\cdot k\} \% p = [1\cdot 2\cdot 3\cdot\ldots(p-1)] \% p$$

$$= [1\cdot 2\cdot 3\cdot\ldots(p-1)]\, k^{p-1} \qquad = (p-1)! \quad \text{"factorial"}$$

$$= (p-1)!\cdot k^{p-1}$$

$$\Rightarrow \quad [(p-1)!\cdot k^{p-1}] \% p = [(p-1)!\cdot 1] \% p$$

$\Rightarrow$ if $(p-1)!$

$$k^{p-1} \% p = 1 \% p = 1$$

FERMAT'S LITTLE THEOREM

How is this useful?

$$7/_f\, 5 = 7 \cdot_f 5^{-1} = 7 \cdot_f (5^{-1} \cdot_f 1) \overset{\text{Fermat w/ } k=5}{=} 7 \cdot_f (5^{-1} \cdot 5^{p-1})$$

$$= 7 \cdot_f (5^{p-2})$$

$$\text{if } p = 11 \quad = 7 \cdot_f (5^{11-2})$$

$$= 7 \cdot_f (5^9)$$

$\Rightarrow$ This enables us to compute

- division
- multiplicative inverses: $a^{-1} = a^{p-2}$ if $a \in \mathbb{F}_p$.

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"

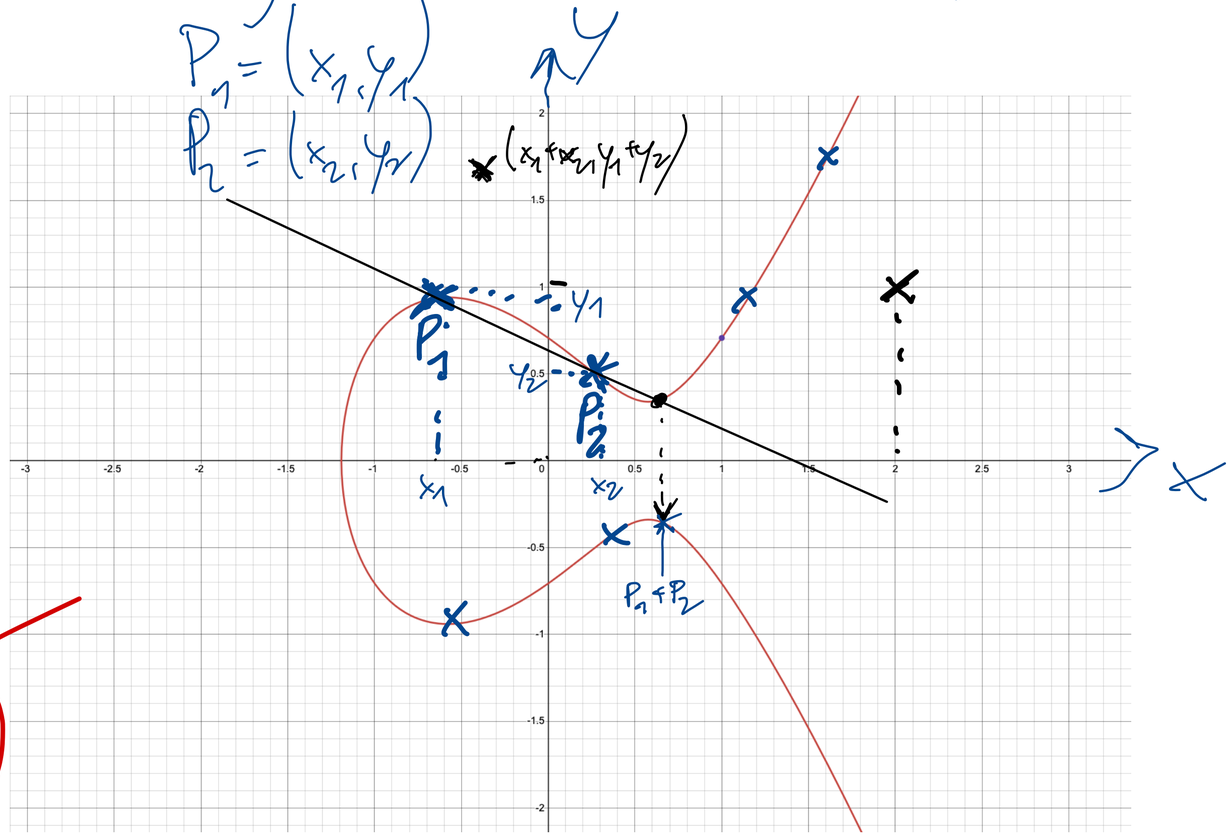
Q: Is $(x,y) = (2,1)$ a point on $S_{a,b}$?

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

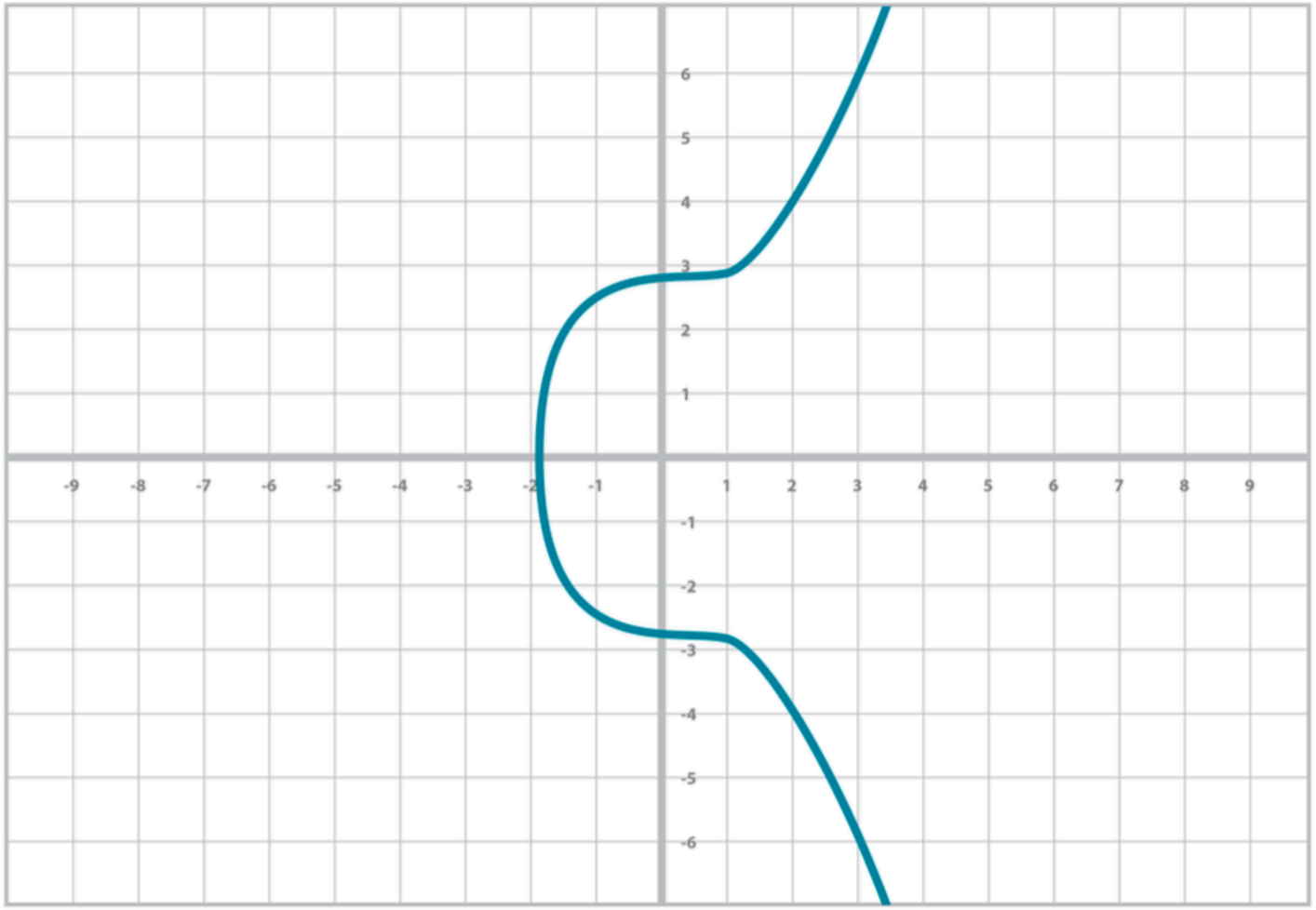
RHS: $x^3 + ax + b = 2^3 + a \cdot 2 + 5$

$a=0,5=7$ $= 8 + 2a + b$

$= 15$



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 $b = 7$.

ELLIPTIC CURVES

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

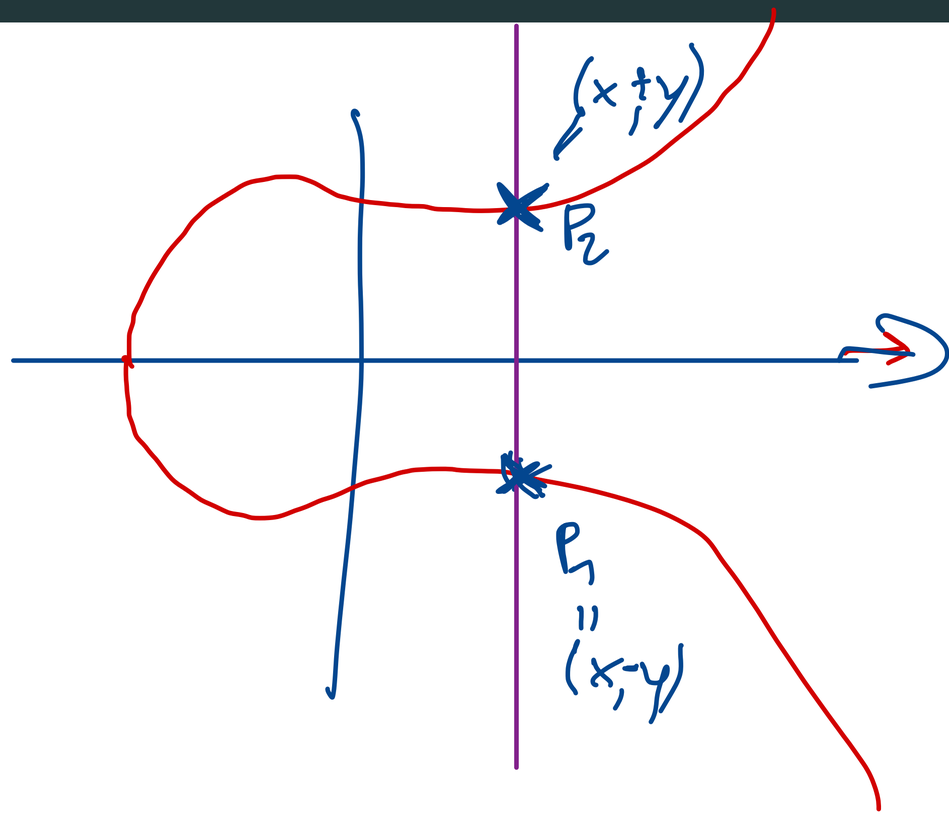
Theorem: (Special case of Bézout's thm.)

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)

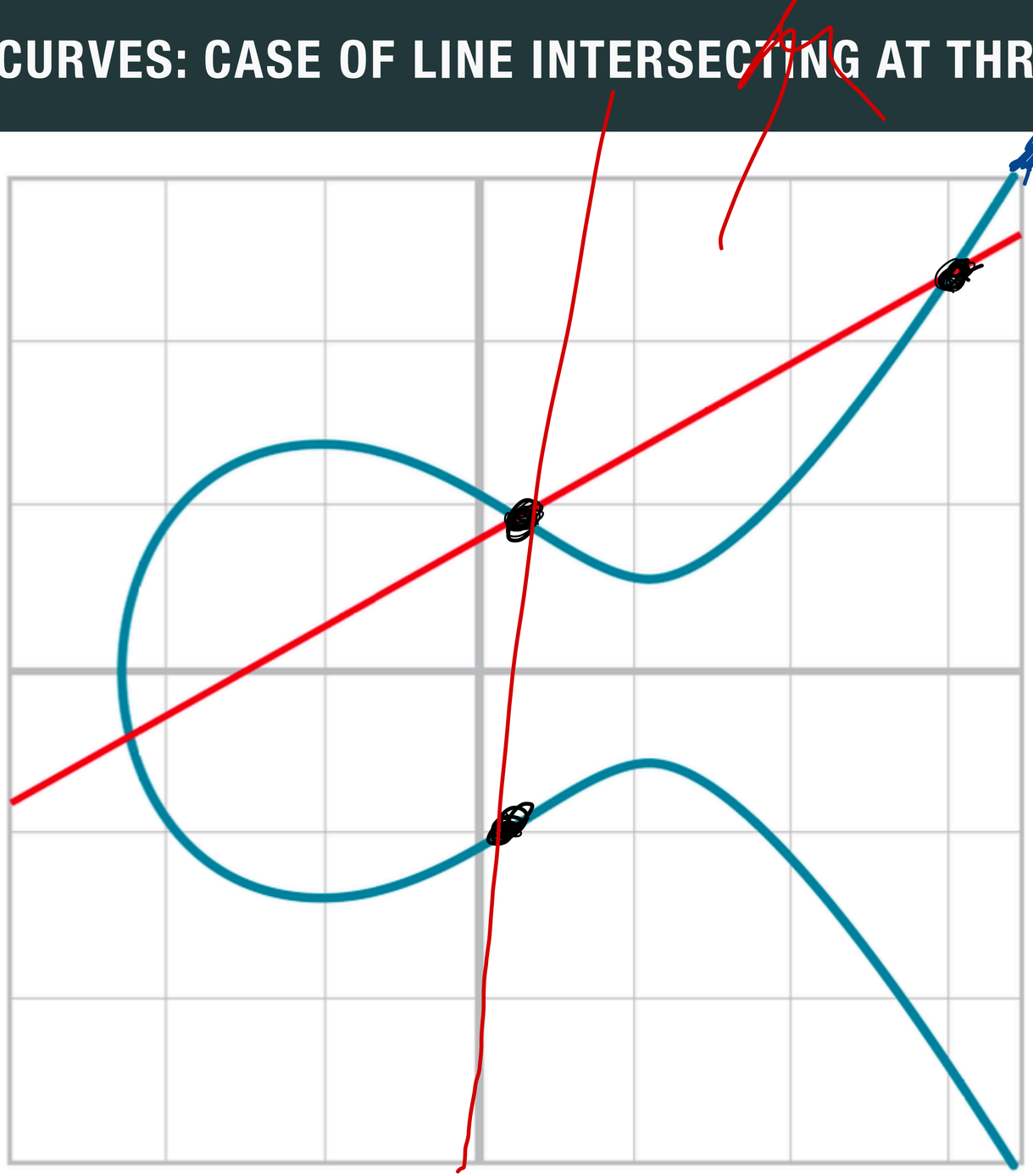
POINT ADDITION ON ELLIPTIC CURVES

Case (c): We define: $P_1 + P_2 = O$

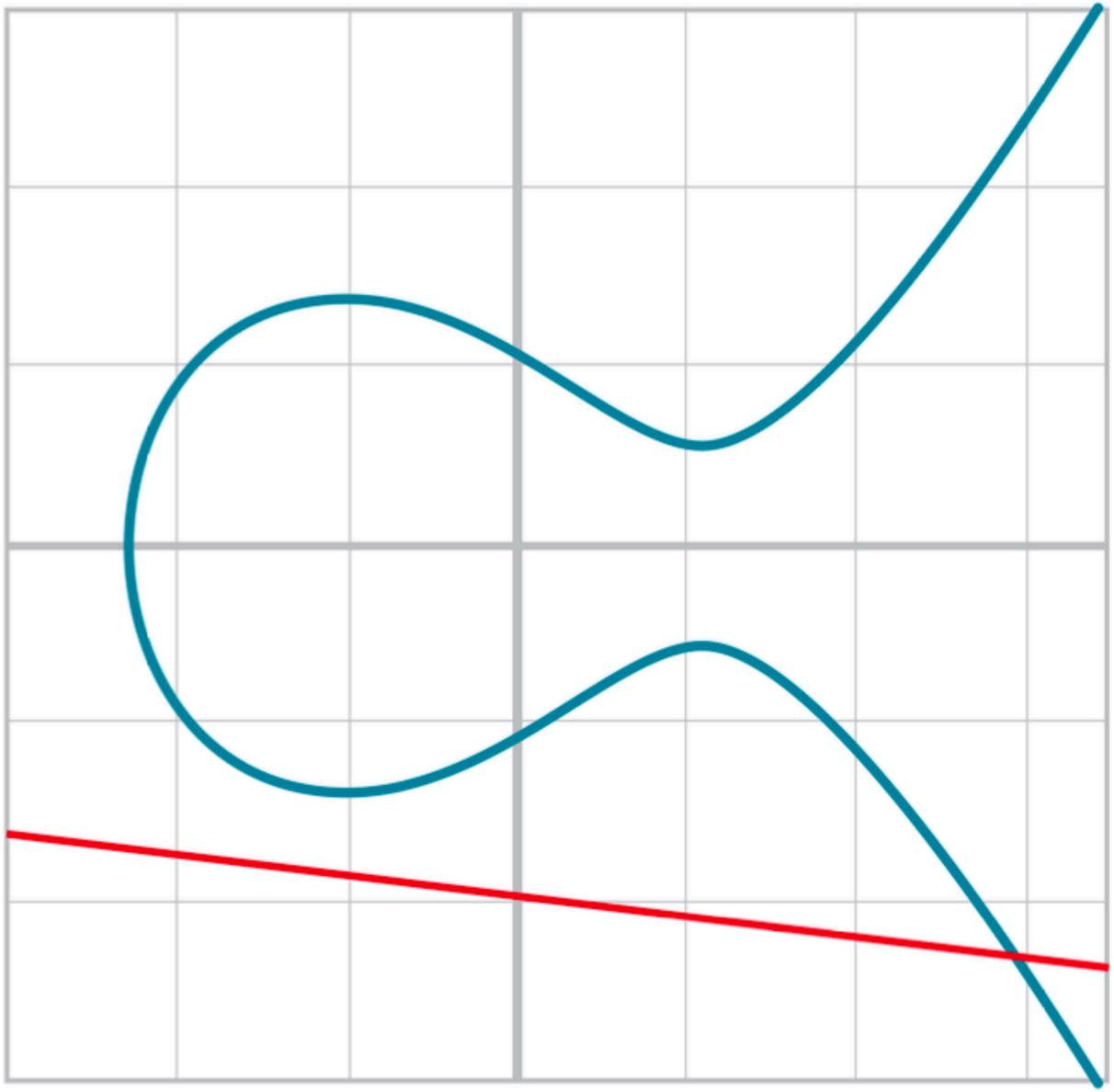
"O" is "point at infinity"



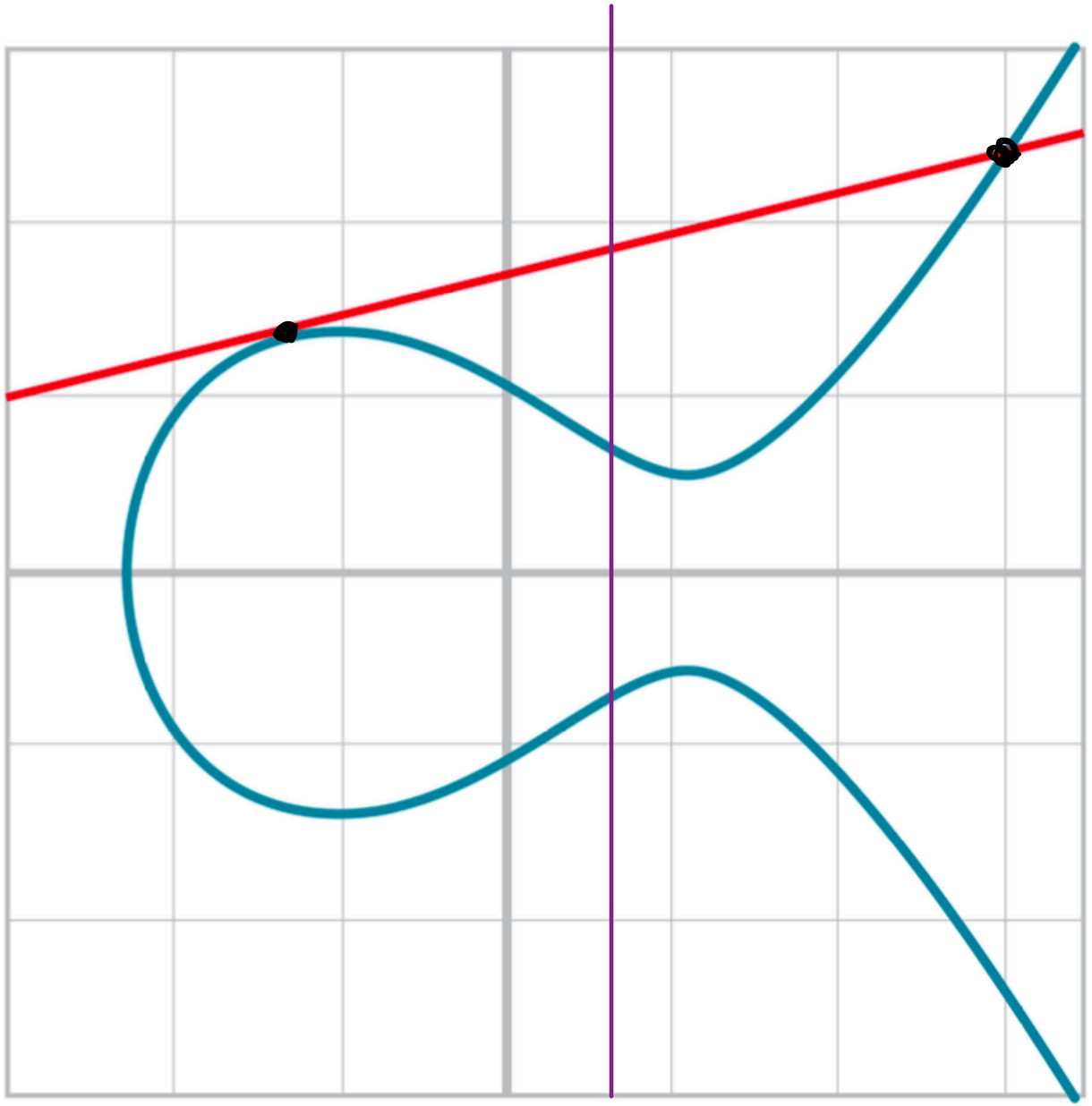
LINES AND ELLIPTIC CURVES: CASE OF LINE INTERSECTING AT THREE POINTS



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



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



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

If $(x, y) \in S_{a,b}$

$\Rightarrow (x, -y) \in S_{a,b}$

POINT ADDITION ON ELLIPTIC CURVES

$P_1 + O = P_1$

$P_1 + (-P_1) = O$