A Course on
Introduction to Arithmetic Dynamics

Mathematics Department
Khon Kaen University

Introduction Elliptic Curves

Chatchawan Panraksa

MUIC

May 26, 2023

Agenda

Introduction

Consider the curve $C : x^2 - 7y^2 = 2$.

Introduction

Consider the curve $C : x^2 - 7y^2 = 2$.

- Is there an integral point on C?

Introduction

Consider the curve $C : x^2 - 7y^2 = 2$.

- Is there an integral point on C?
  Yes! $(3, 1)$

Introduction

Consider the curve $C : x^2 - 7y^2 = 2$.

- Is there an integral point on C?
  Yes! $(3, 1)$
- Can we find all rational points on C?

Introduction

Consider the curve $C : x^2 - 7y^2 = 2$.

- Is there an integral point on C?
  Yes! $(3, 1)$
- Can we find all rational points on C?
  Yes! "Chord-Tangent method"

Notation: For a curve $C : P(x, y) = 0$ defined over a field K.
$C(K) = \{(x_0, y_0) \in K \times K : P(x_0, y_0) = 0\}$
p-adic norm Let p be a prime number and $x = \frac{a}{b}p^n \in \mathbb{Q}$ where a, b, p are relatively prime.
The $p-$adic norm of Q is defined as $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$
$|x|_p = p^{-n}$ ($|0|_p = 0$).
Note that $|\cdot|_p$ is a norm.
Moreover $|x + y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$ (it is non-archimedean).

Theorem (Hasse-Minkowski)

Let C be a quadratic curve. Then $C(\mathbb{Q}) \neq \emptyset$ if and only if $C(\mathbb{Q}_p) \neq \emptyset$ for all places p of $\mathbb{Q}$.In this case $C(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$, i.e., $C(\mathbb{Q})$ is infinite.

Diophantine Equations

$f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$, R is a ring or field
$(R = \mathbb{Z}, \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_q, \mathbb{F}_q(t), \ldots)$
Diophantine equation: $f(x_1, x_2, \ldots, x_n) = 0$
Examples

- $x - 1 = 0, R = \mathbb{R}$
- $x^2 + y^2 - 1 = 0, R = \mathbb{Q}$
- $x^4 + y^4 - z^4 = 0, R = \mathbb{Z}$ (Fermat's Last Theorem, $n = 4$)
- $E(\mathbb{Q}) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$

More examples

- $x^3 + y^3 + z^3 = 29, x, y, z \in \mathbb{Z}$?

More examples

- $x^3 + y^3 + z^3 = 29, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (3, 1, 1)$

More examples

- $x^3 + y^3 + z^3 = 29, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (3, 1, 1)$
- $x^3 + y^3 + z^3 = 30, x, y, z \in \mathbb{Z}$?

More examples

- $x^3 + y^3 + z^3 = 29, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (3, 1, 1)$
- $x^3 + y^3 + z^3 = 30, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (-283059965, -2218888517, 2220422932)$
  (E. Pine, K. Yarbrough, W. Tarrant, M. Beck, suggested by N.Elkies)

More examples

- $x^3 + y^3 + z^3 = 29, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (3, 1, 1)$
- $x^3 + y^3 + z^3 = 30, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (-283059965, -2218888517, 2220422932)$
  (E. Pine, K. Yarbrough, W. Tarrant, M. Beck, suggested by N.Elkies)
- $x^3 + y^3 + z^3 = 33$?

More examples

- $x^3 + y^3 + z^3 = 29, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (3, 1, 1)$
- $x^3 + y^3 + z^3 = 30, x, y, z \in \mathbb{Z}$?
  Solution: $(x, y, z) = (-283059965, -2218888517, 2220422932)$
  (E. Pine, K. Yarbrough, W. Tarrant, M. Beck, suggested by N.Elkies)
- $x^3 + y^3 + z^3 = 33$?
  Solution:??? (Unknown)

Hilbert's tenth problem

Hilbert's tenth problem: Does there exist an algorithm to return YES or NO according to whether there exist integers $a_1, a_2, \ldots, a_n$ such that $f(a_1, a_2, \ldots, a_n) = 0$, where $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$?

Theorem (Davis-Putnam-Robinson 1961, Matiyasevich 1970)

There is no such algorithm.

Hilbert's tenth problem for $\mathbb{Q}$

Problem (B. Poonen, 2003):
How about $f(x_1, x_2, \ldots, x_n) \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$?

What is an Elliptic Curve?

- An elliptic curve is not an ellipse! The name is a historical misnomer stemming from the theory of elliptic integrals.
- Formally, an elliptic curve E over a field K is a smooth projective curve of genus one defined over K with a specified K-rational point.
- In simpler terms, when we consider real numbers, an elliptic curve is a set of points (x, y) satisfying the equation $y^2 = x^3 + ax + b$, where a and b are real numbers, such that the cubic polynomial on the right-hand side, $x^3 + ax + b$, has distinct roots. This condition ensures that the curve is non-singular, i.e., it has no cusps or self-intersections.
- The equation $y^2 = x^3 + ax + b$ is called the Weierstrass equation. Most elliptic curves arise in this form in the complex plane.
- An elliptic curve also contains a "point at infinity". In the context of projective geometry, this point serves as an identity for the group operation on the curve.

Definition of an Elliptic Curve over a Field K

Definition

An **elliptic curve** over a field K is a curve having an equation of the form $y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$, where $a_1, a_2, a_3, a_4, a_5 \in K$.
If $char(K) \neq 2, 3$, then it can be transformed to

$$E : y^2 = x^3 + Ax + B, A, B \in K.$$

If $4A^3 + 27B^2 \neq 0$, then E is called **non-singular**.

Definition of an Elliptic Curve over a Field K

Definition

An **elliptic curve** over a field K is a curve having an equation of the form $y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$, where $a_1, a_2, a_3, a_4, a_5 \in K$.
If $char(K) \neq 2, 3$, then it can be transformed to

$$E : y^2 = x^3 + Ax + B, A, B \in K.$$

If $4A^3 + 27B^2 \neq 0$, then E is called **non-singular**.

Why $4A^3 + 27B^2$?

Definition of an Elliptic Curve over a Field K

Definition

An **elliptic curve** over a field K is a curve having an equation of the form $y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$, where $a_1, a_2, a_3, a_4, a_5 \in K$.
If $char(K) \neq 2, 3$, then it can be transformed to

$$E : y^2 = x^3 + Ax + B, A, B \in K.$$

If $4A^3 + 27B^2 \neq 0$, then E is called **non-singular**.

Why $4A^3 + 27B^2$?
Answer: $Disc_x(x^3 + Ax + B) = 4A^3 + 27B^2$, where
$\Delta_f = Disc_x(f)$ is a **discriminant** of a polynomial $f(x)$.
$f(x) = a_mx^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0, Disc_x(f) = a_m^{2m-2} \prod_{i<j}(r_i - r_j)^2,$

where $r_1, r_2, \ldots, r_m$ are not necessarily distinct roots of $f(x)$.

Resultant

For $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, **resultant** $Res_x(f, g) = |S_{f,g}|$ where $S_{f,g} \in \mathcal{M}_{(m+n)\times(m+n)}$ is the Sylvester matrix of f and g.

Example $f(x) = 2x^2 - 3x + 4, g(x) = -5x^3 + 6x^2 - 7x - 8$

$$S_{f,g} = \begin{bmatrix} 2 & -3 & 4 & 0 & 0 \\ 0 & 2 & -3 & 4 & 0 \\ 0 & 0 & 2 & -3 & 4 \\ -5 & 6 & -7 & -8 & 0 \\ 0 & -5 & 6 & -7 & -8 \end{bmatrix}$$

Equivalently, $Disc_x(f) = \frac{(-1)^{\frac{m(m-1)}{2}}}{a_m} Res_x(f, f')$.

Reducing an Elliptic Curve

To simplify calculations and apply various algorithms, it is beneficial to reduce an elliptic curve to the form $y^2 = x^3 + ax + b$.

- Start with a general form of an elliptic curve:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- We set $y' = y + \frac{a_1}{2}x + \frac{a_3}{2}$ and $x' = x + \frac{a_2}{3}$. Then the curve can be reduced to

$$E : (y')^2 = (x')^3 + A(x') + B$$

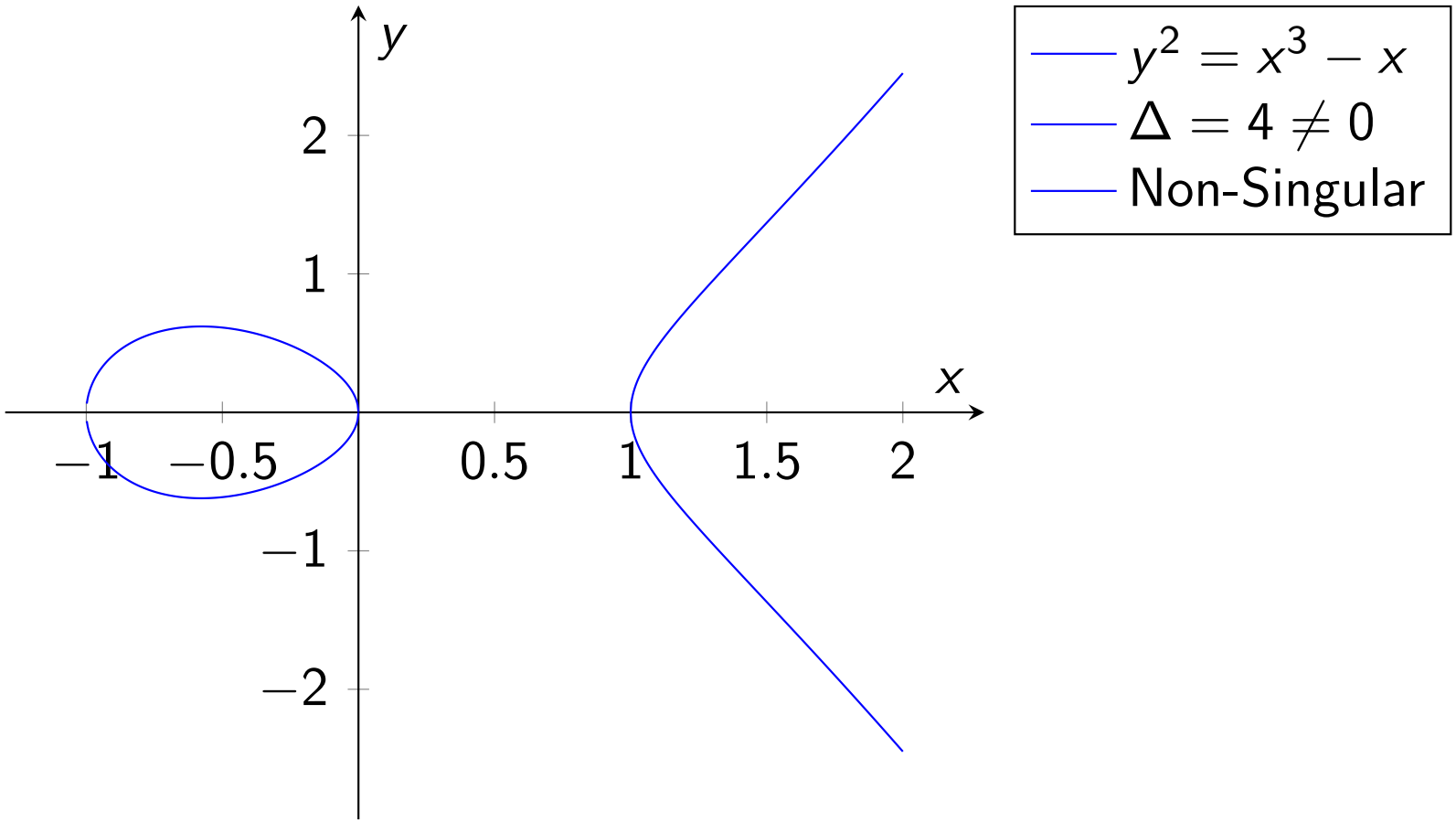
An elliptic curve having an equation of the form

$$y^2 = x^3 + Ax + B$$

is said to be in **reduced Weierstrass form**.

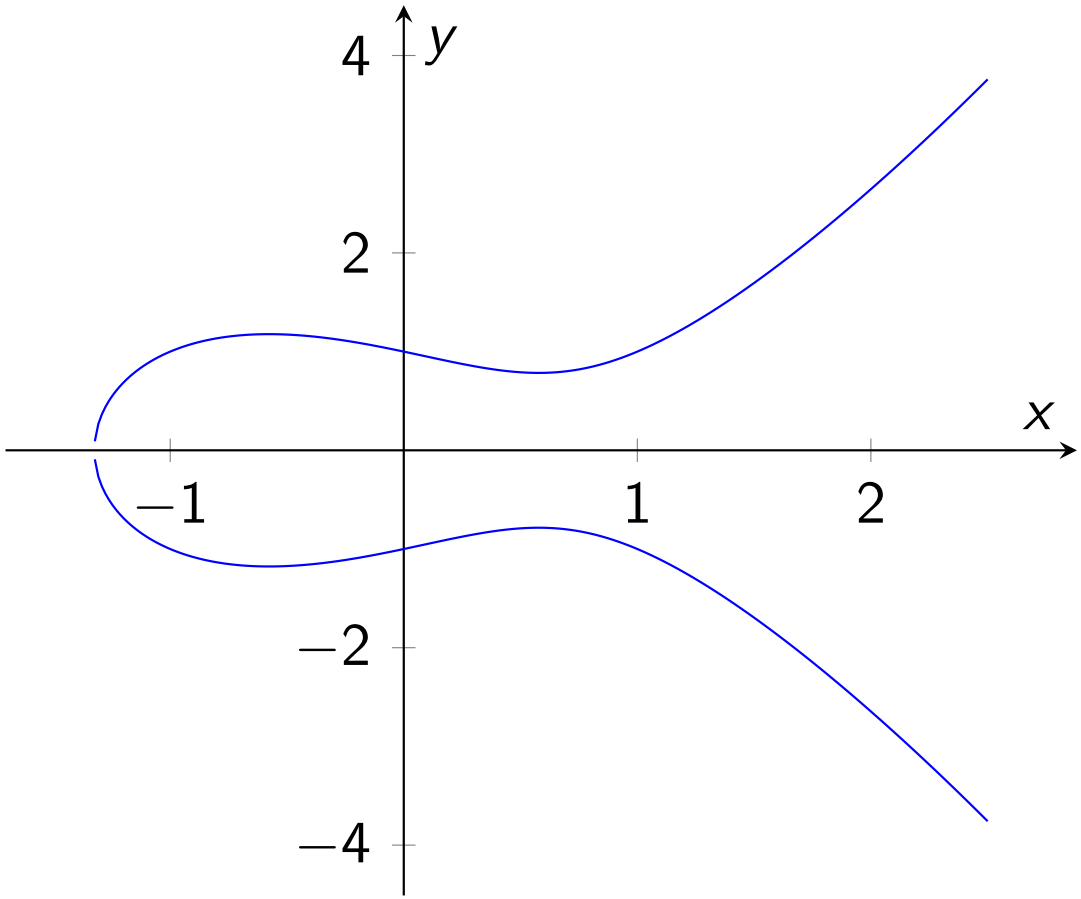
Example 1

Consider the elliptic curve defined by the equation $y^2 = x^3 - x$. This curve includes points where both x and y are real numbers and the equation holds true. The curve is symmetric about the x-axis, and has two components, crossing the x-axis at (-1,0), (0,0), and (1,0).



Example 2

Consider the elliptic curve defined by the equation $y^2 = x^3 - x + 1$. This curve includes points where both x and y are real numbers and the equation holds true. The curve is symmetric about the x-axis, and has one component.

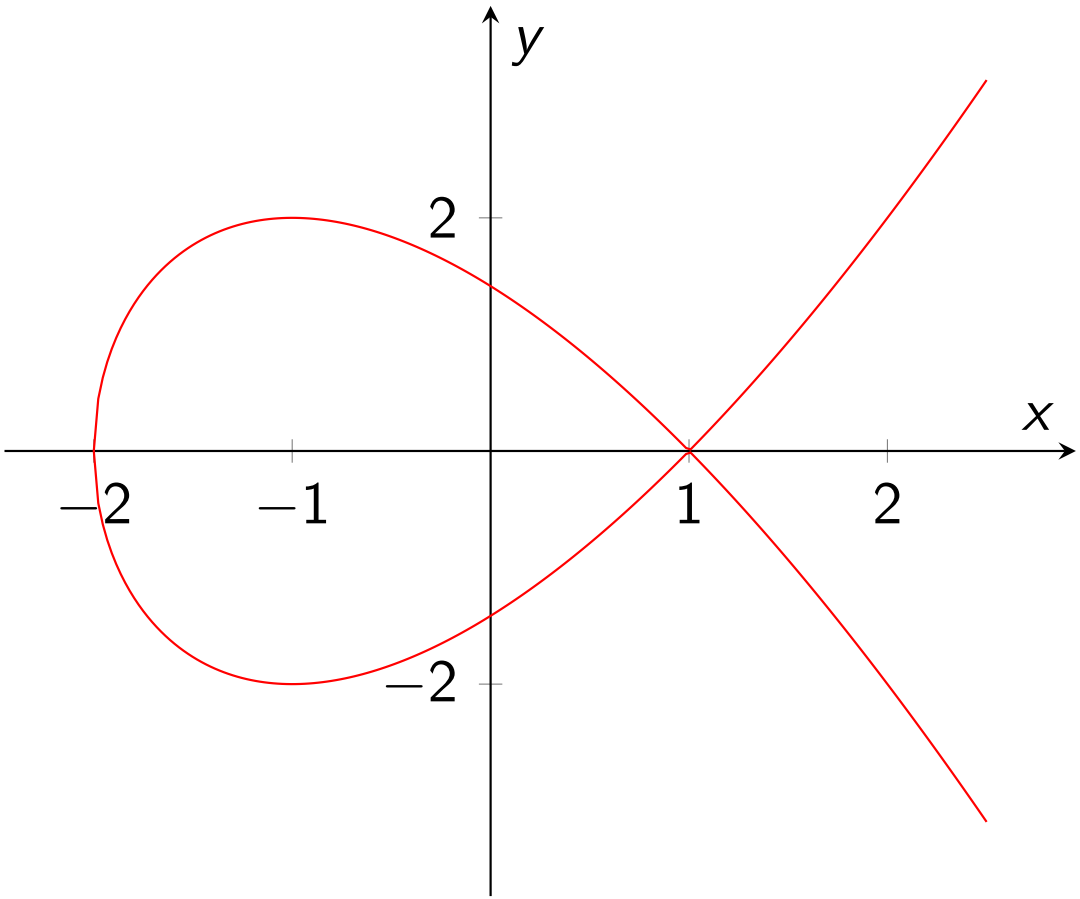


$y^2 = x^3 - x + 1$

$\Delta = -23 \neq 0$

Example 3

Consider the elliptic curve defined by the equation $y^2 = x^3 - 3x + 2$. This curve includes points where both x and y are real numbers and the equation holds true. The curve is symmetric about the x-axis, and has a self-intersection point at $(1, 0)$.



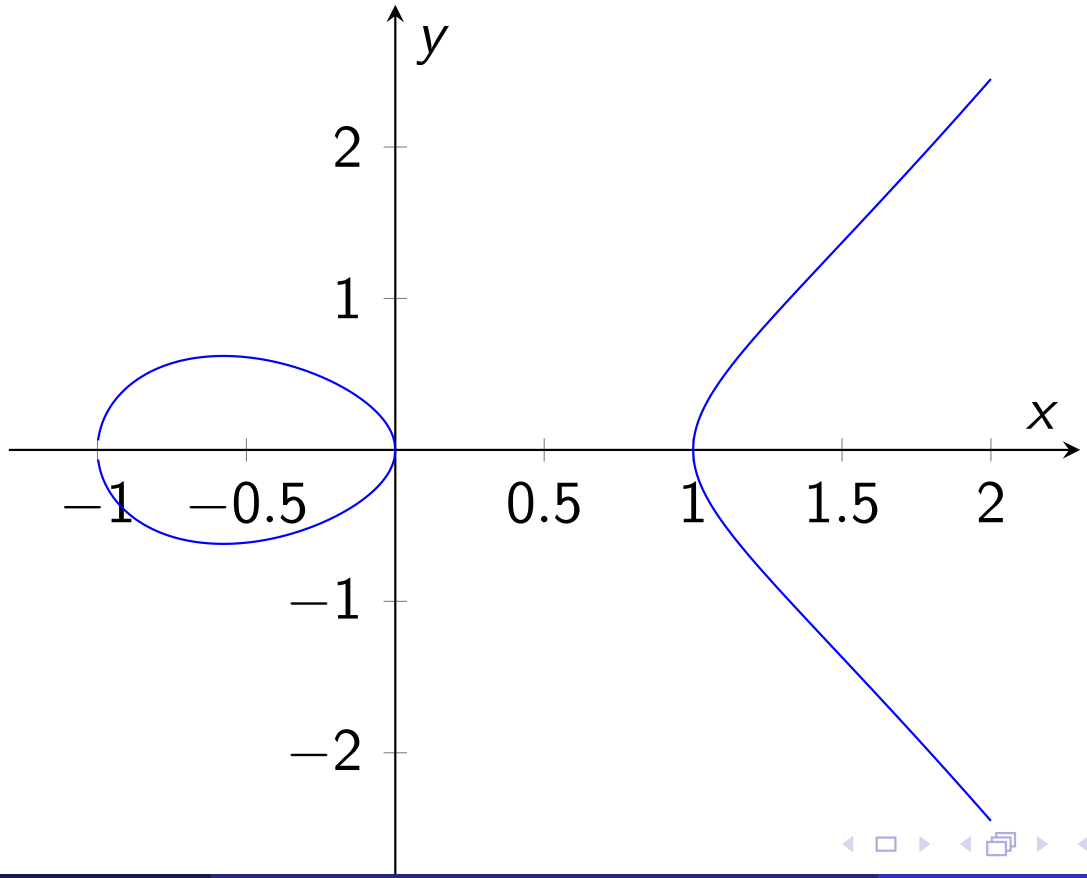
$y^2 = x^3 - 3x + 2$

$\Delta = 0$

Properties of Elliptic Curves: Symmetry

An elliptic curve defined by the equation $y^2 = x^3 + ax + b$ is symmetric about the x-axis.

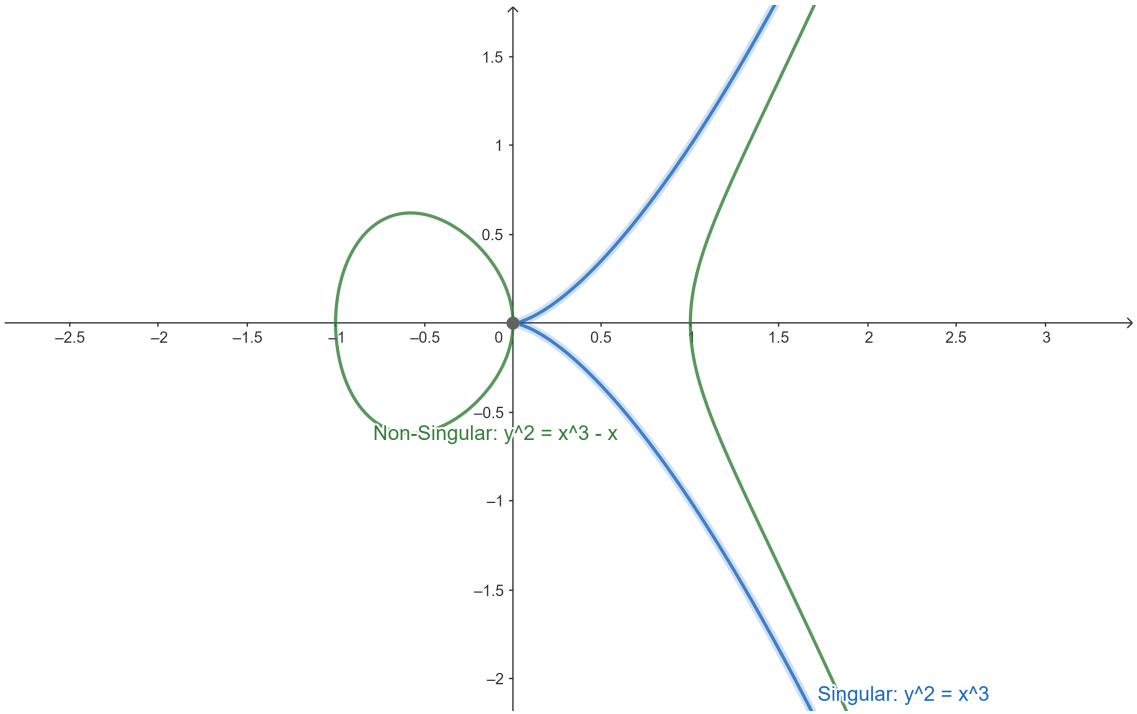
- If (x, y) is a point on the curve, then $(x, -y)$ is also a point on the curve.
- This property can be visually observed in the graphs of elliptic curves.



Properties of Elliptic Curves: Non-Singularity

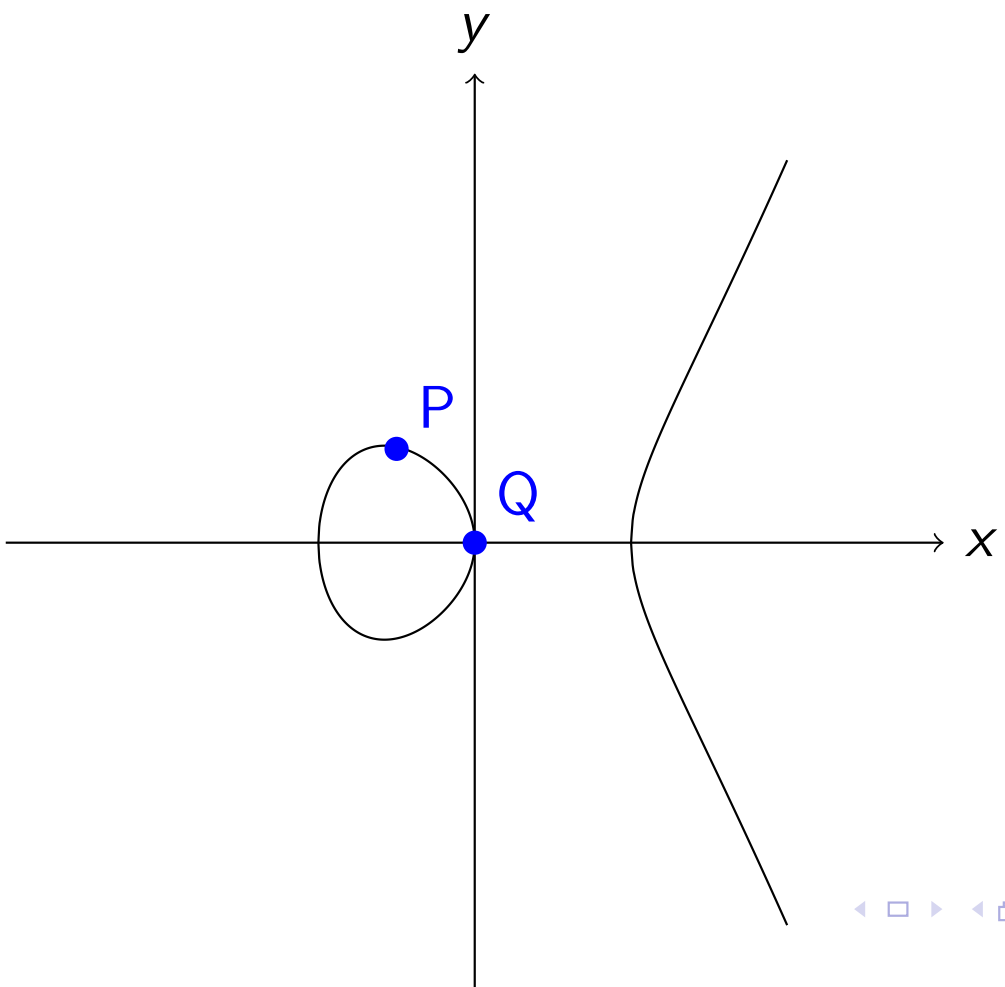
Elliptic curves are non-singular - they have no cusps, self-intersections, or isolated points.

- In terms of the Weierstrass equation, this means that the cubic polynomial $x^3 + Ax + B$ has distinct roots.
- This property ensures that the curve is smooth everywhere, which is essential for the group law operation.



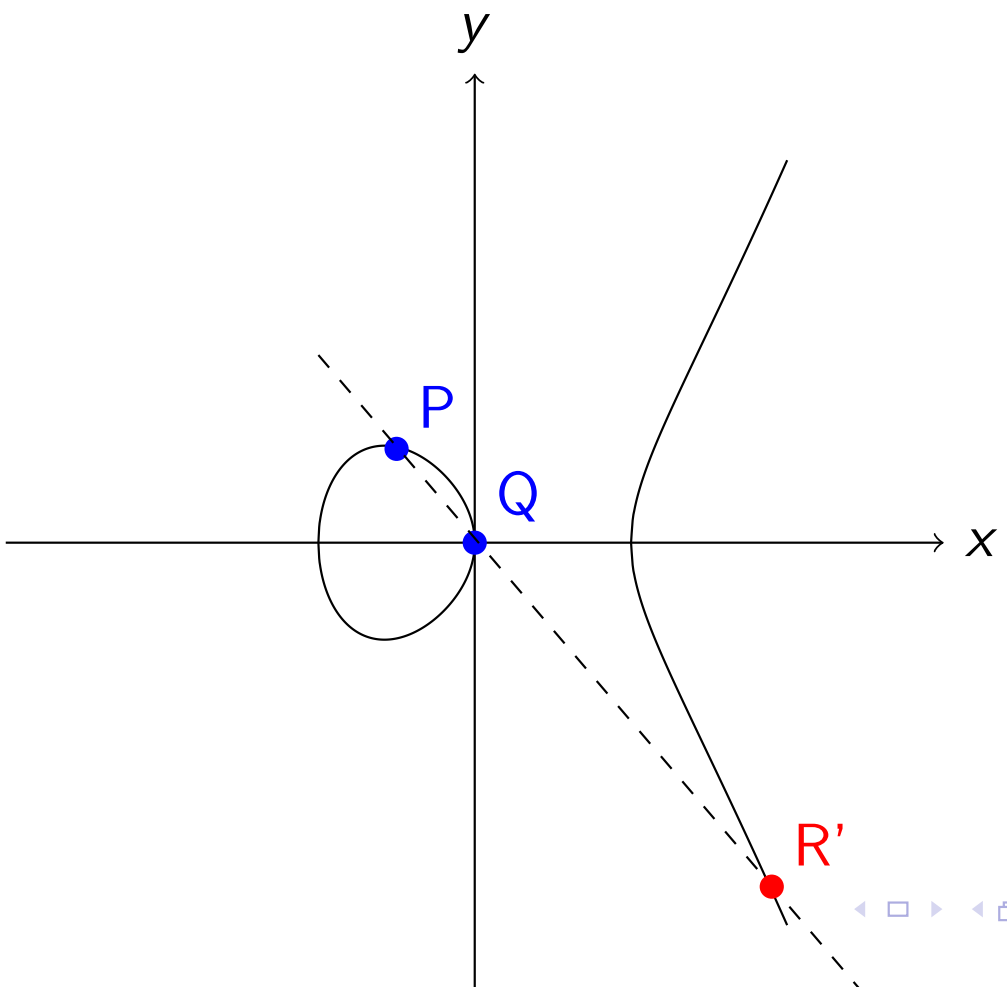
Addition of Points on Elliptic Curves

- Elliptic curves form a group under a geometric operation called point addition.
- Given two points P and Q on the curve, the line passing through P and Q intersects the curve at a third point R.



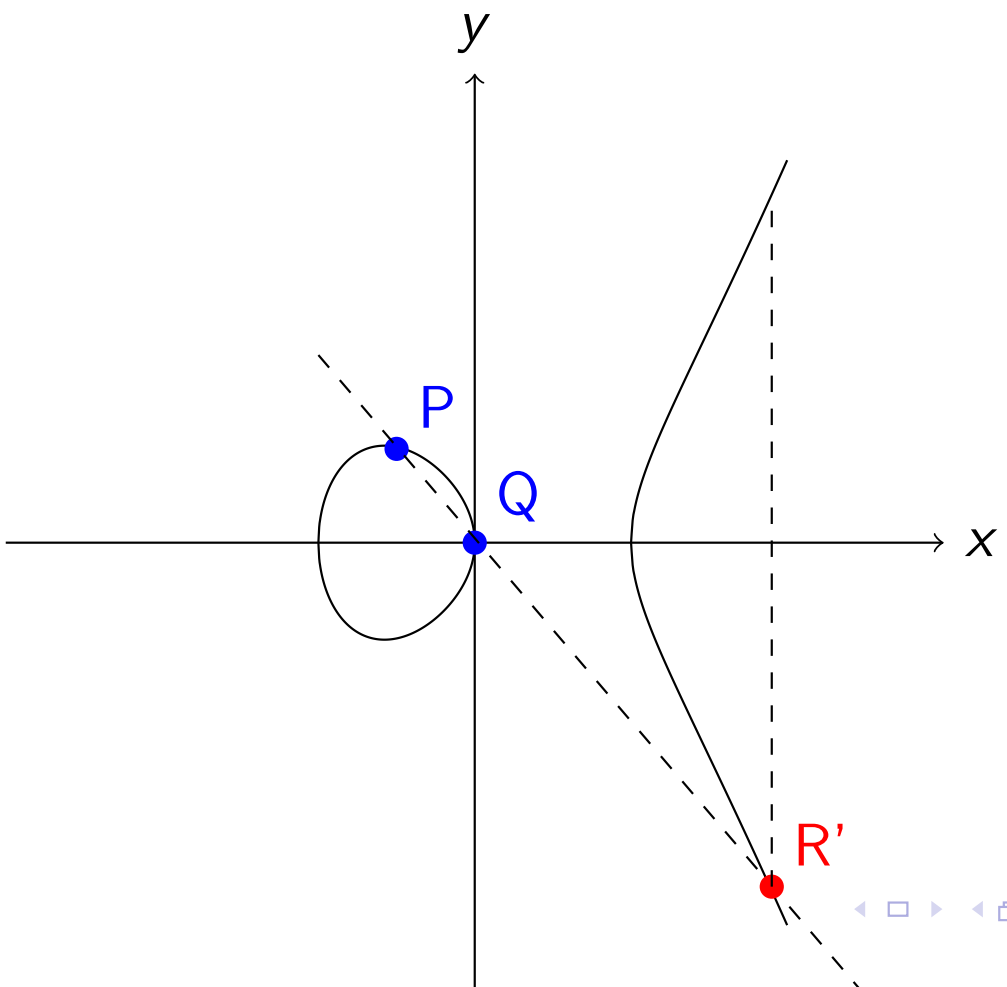
Addition of Points on Elliptic Curves

- Elliptic curves form a group under a geometric operation called point addition.
- Given two points P and Q on the curve, the line passing through P and Q intersects the curve at a third point R.



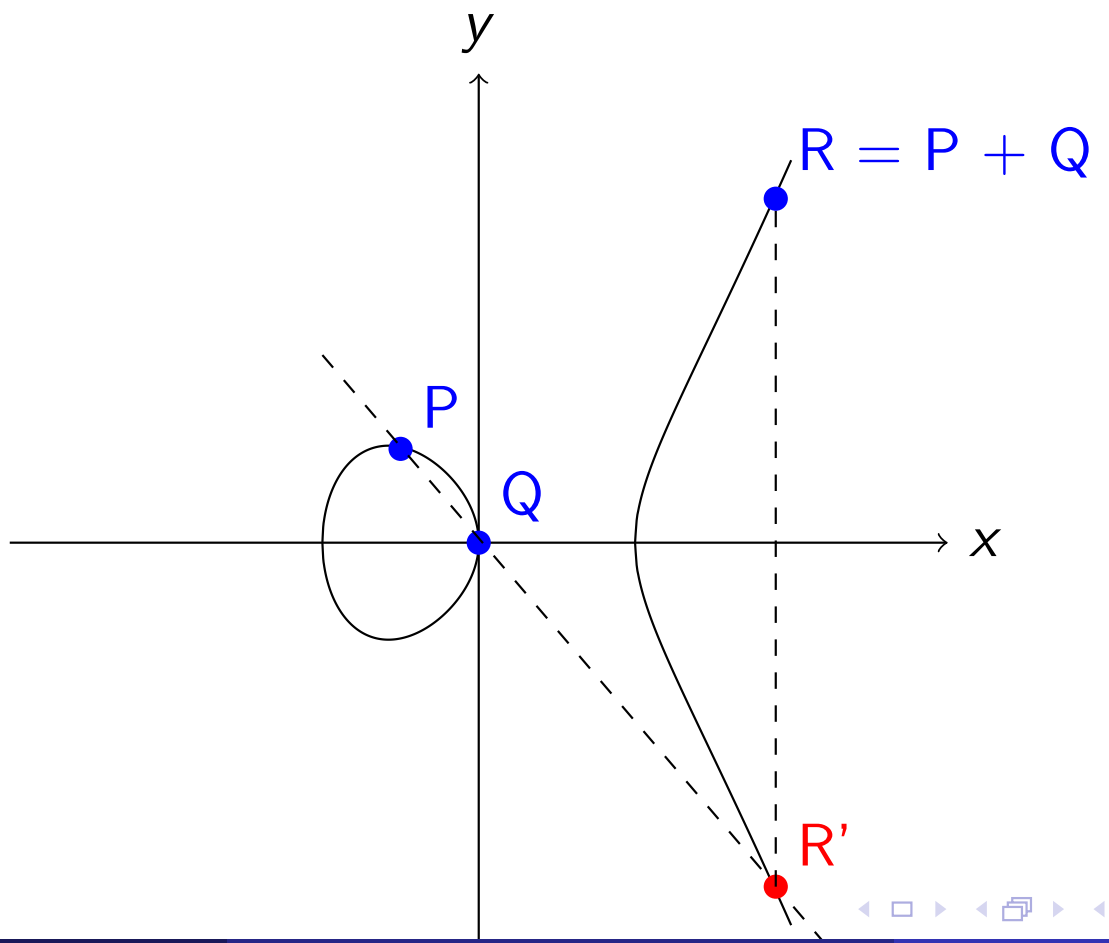
Addition of Points on Elliptic Curves

- Elliptic curves form a group under a geometric operation called point addition.
- Given two points P and Q on the curve, the line passing through P and Q intersects the curve at a third point R.

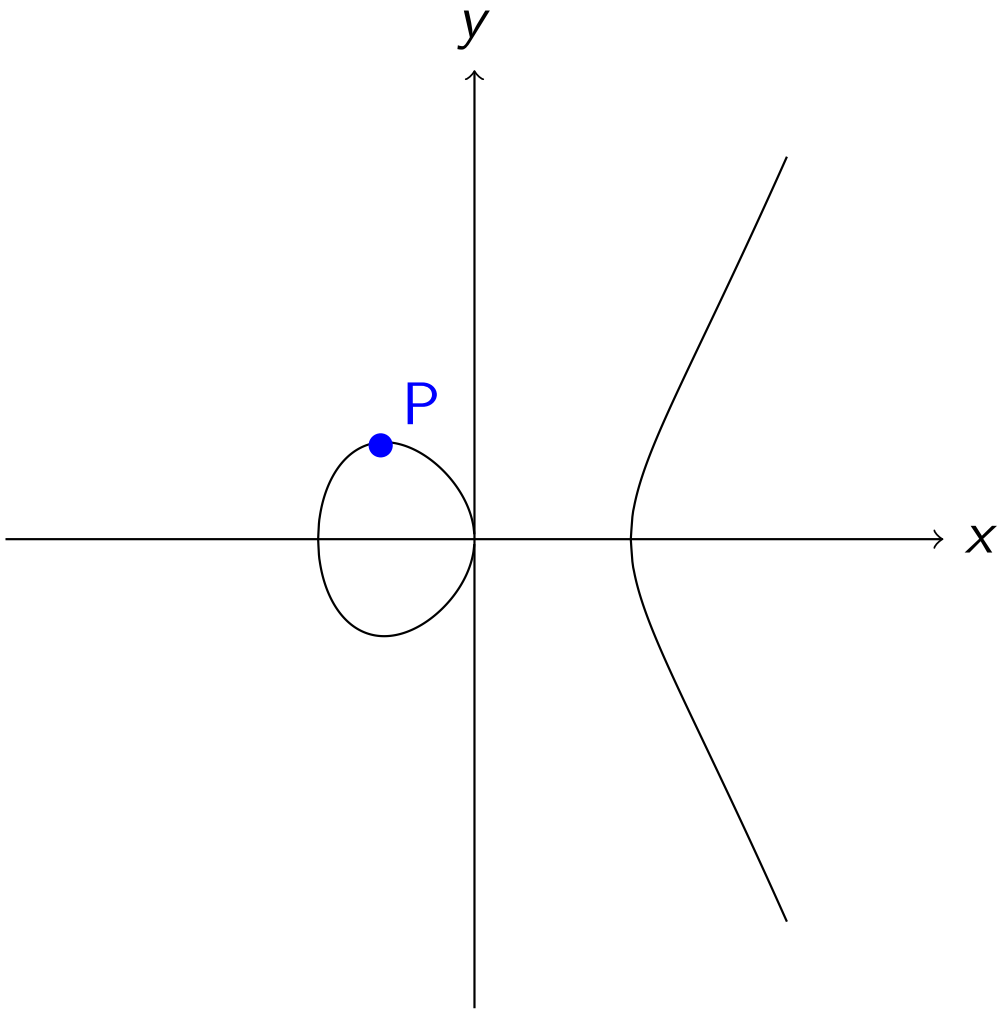


Addition of Points on Elliptic Curves

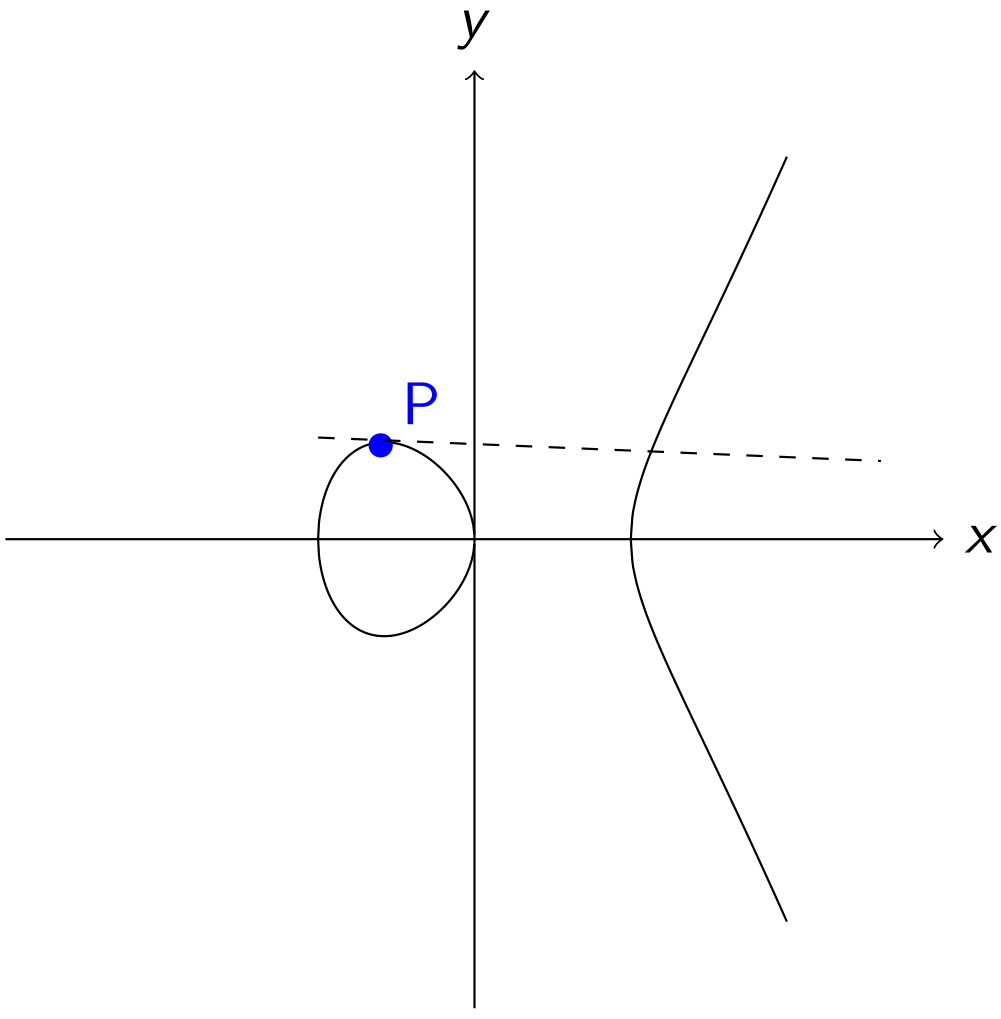
- Elliptic curves form a group under a geometric operation called point addition.
- Given two points P and Q on the curve, the line passing through P and Q intersects the curve at a third point R.



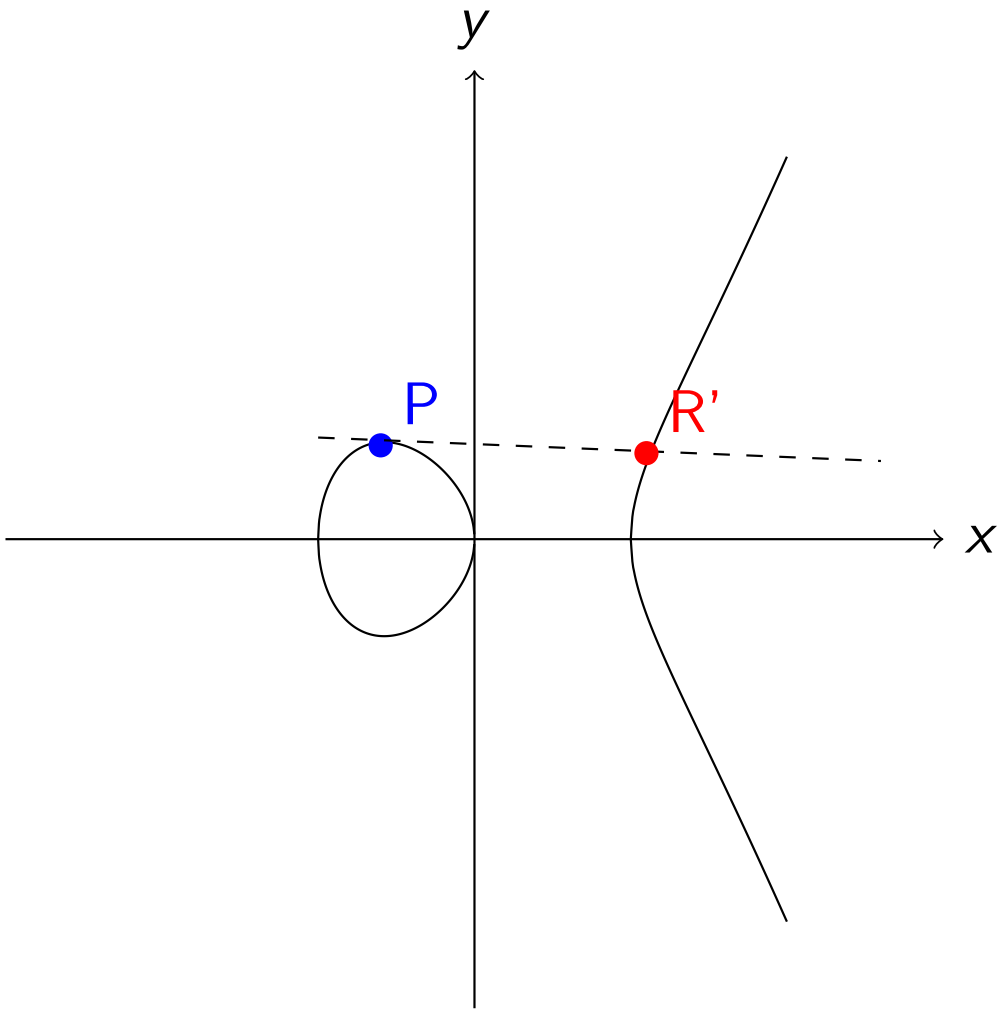
$P + P$?



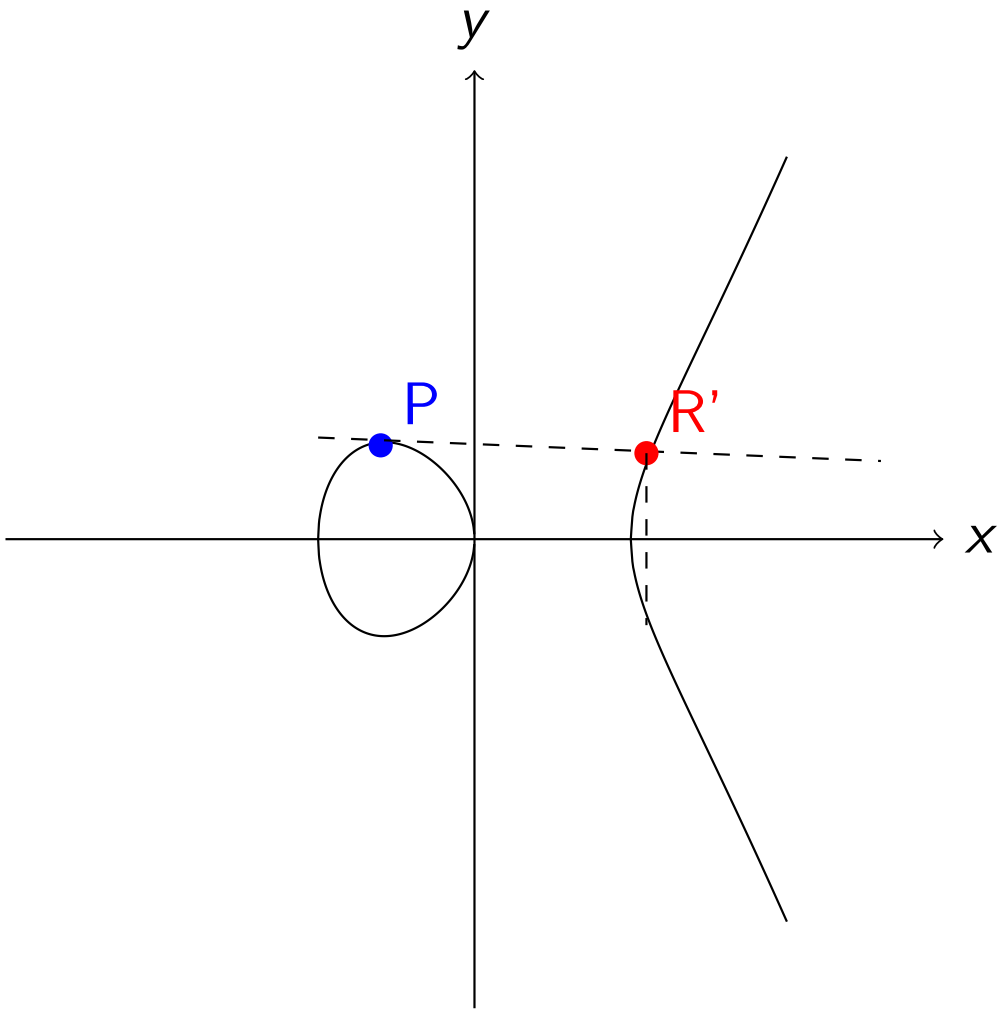
$P + P$?



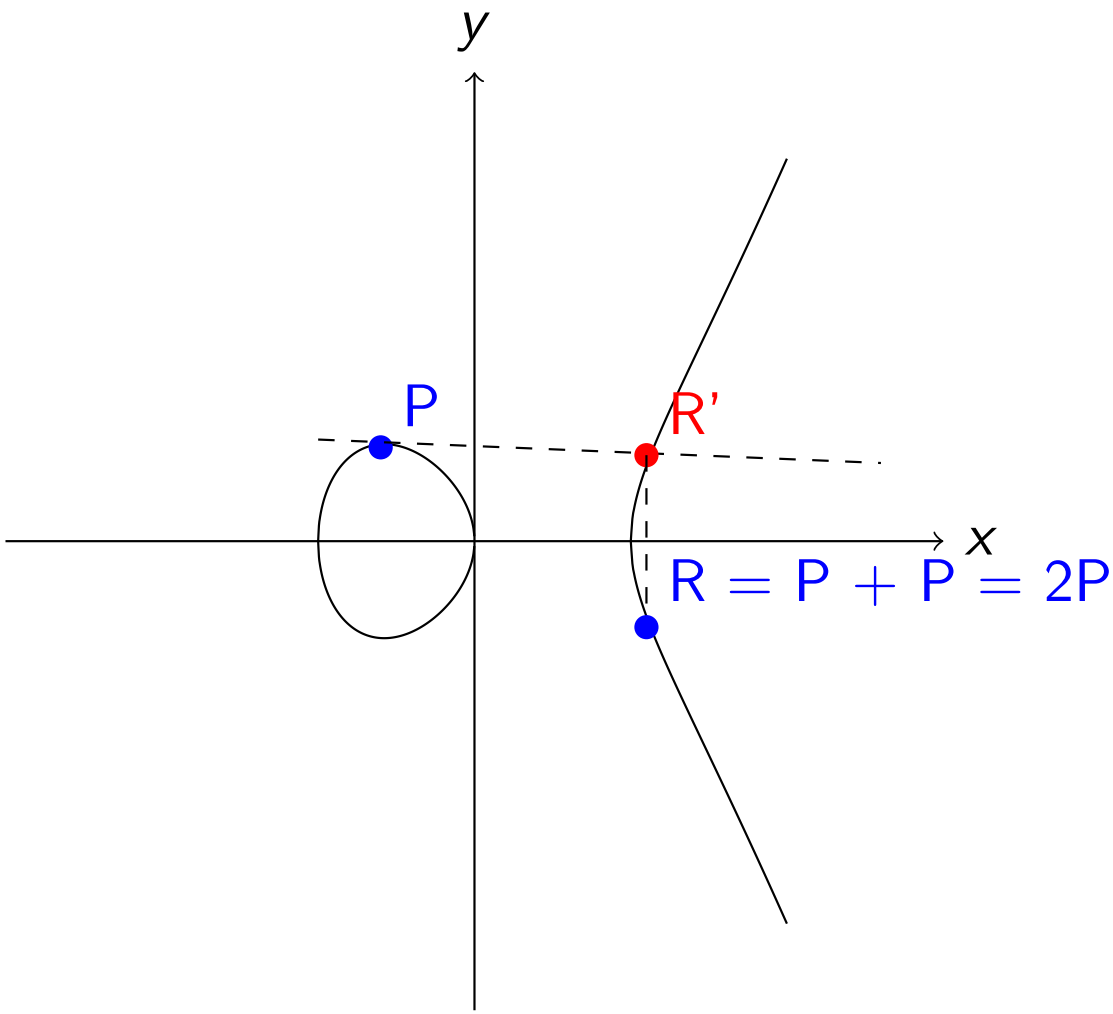
$P + P$?



$P + P$?

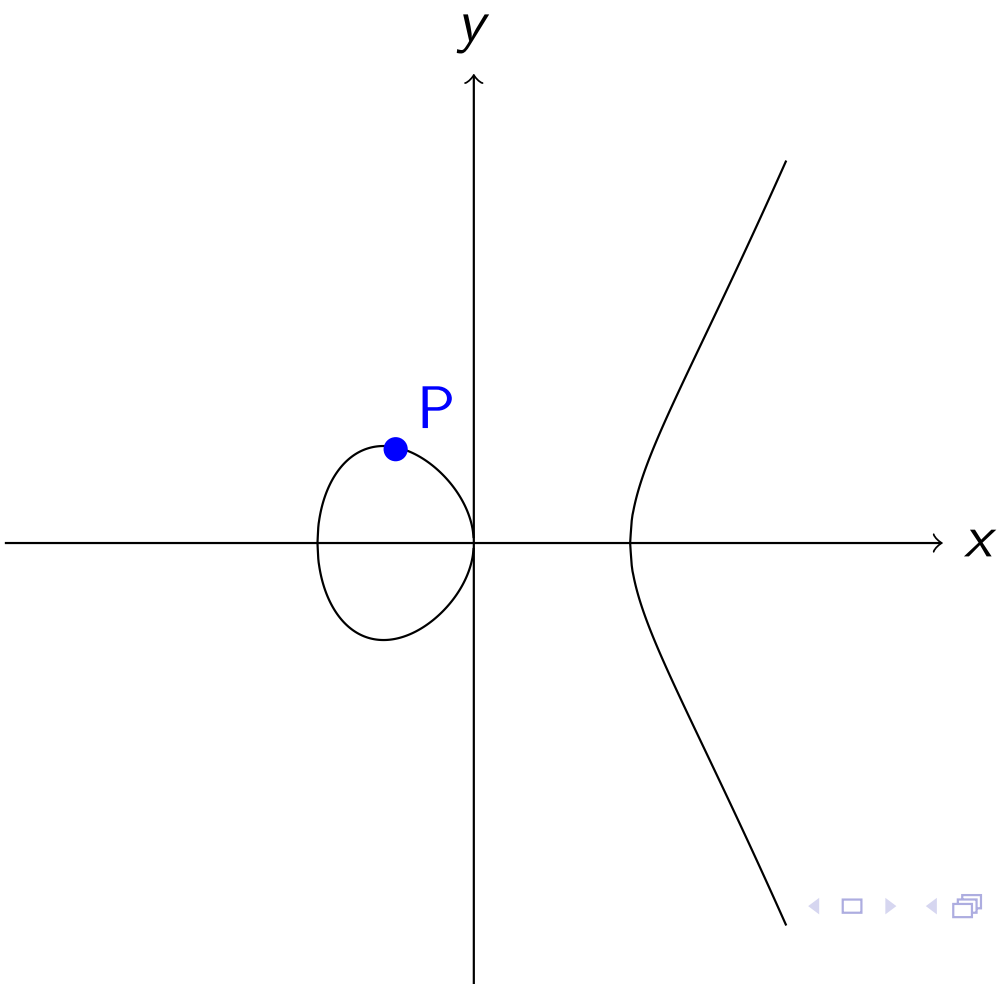


$P + P$?



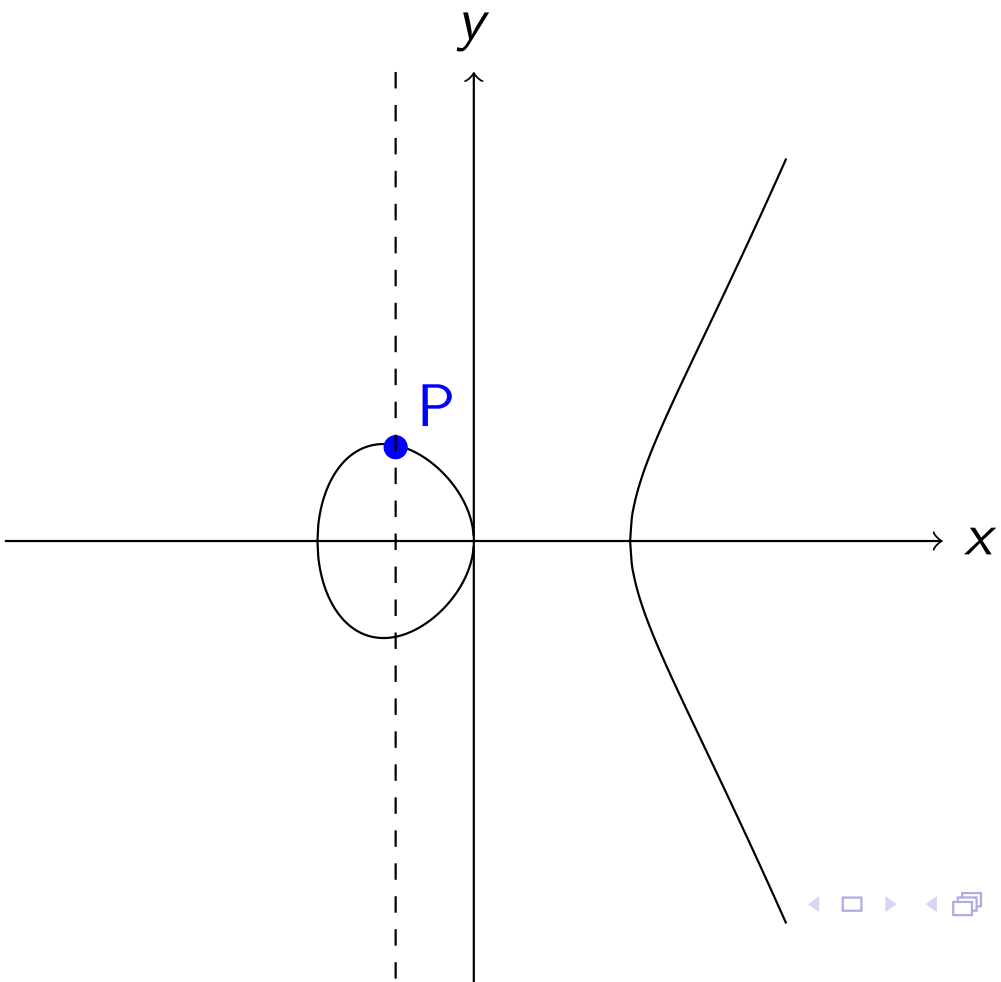
Point at Infinity

- **Point at Infinity**: In the projective plane, all lines intersect, so the vertical line through any point P on the curve intersects the curve at a "point at infinity". This point serves as the identity element of the group.



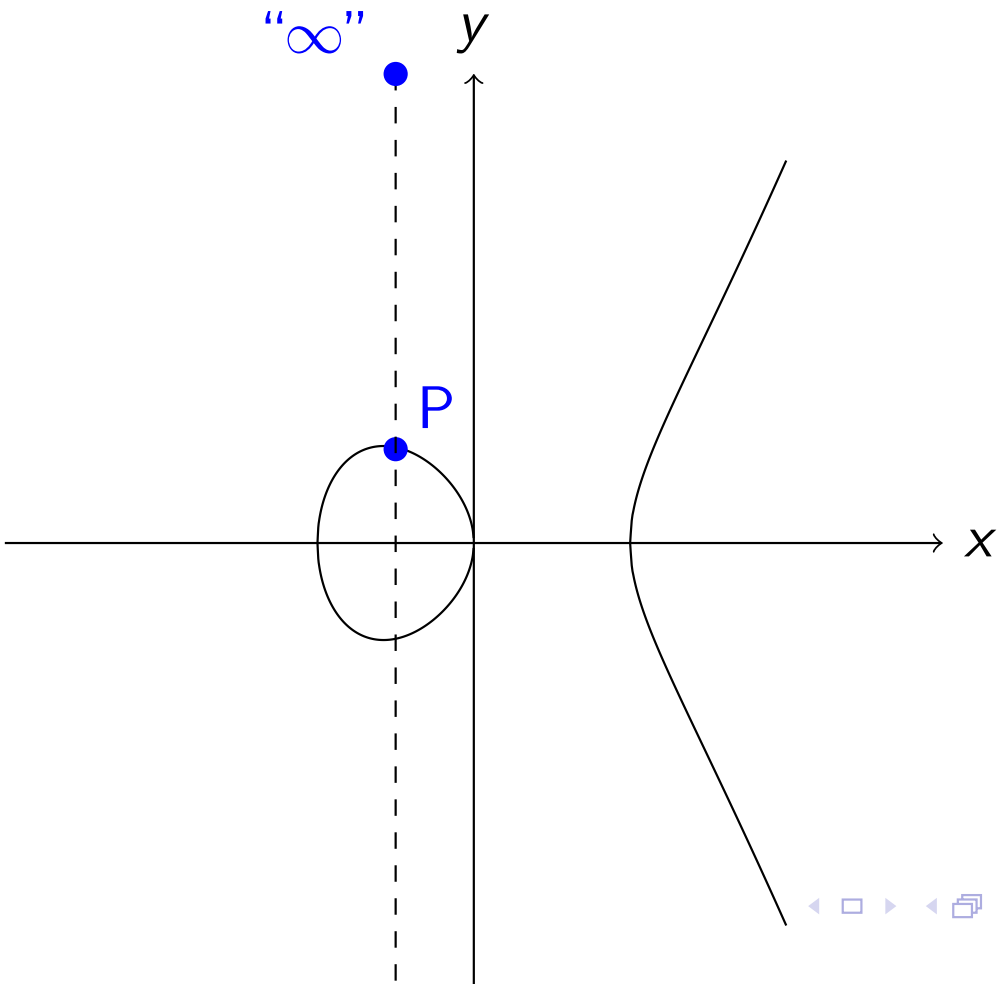
Point at Infinity

- **Point at Infinity**: In the projective plane, all lines intersect, so the vertical line through any point P on the curve intersects the curve at a "point at infinity". This point serves as the identity element of the group.



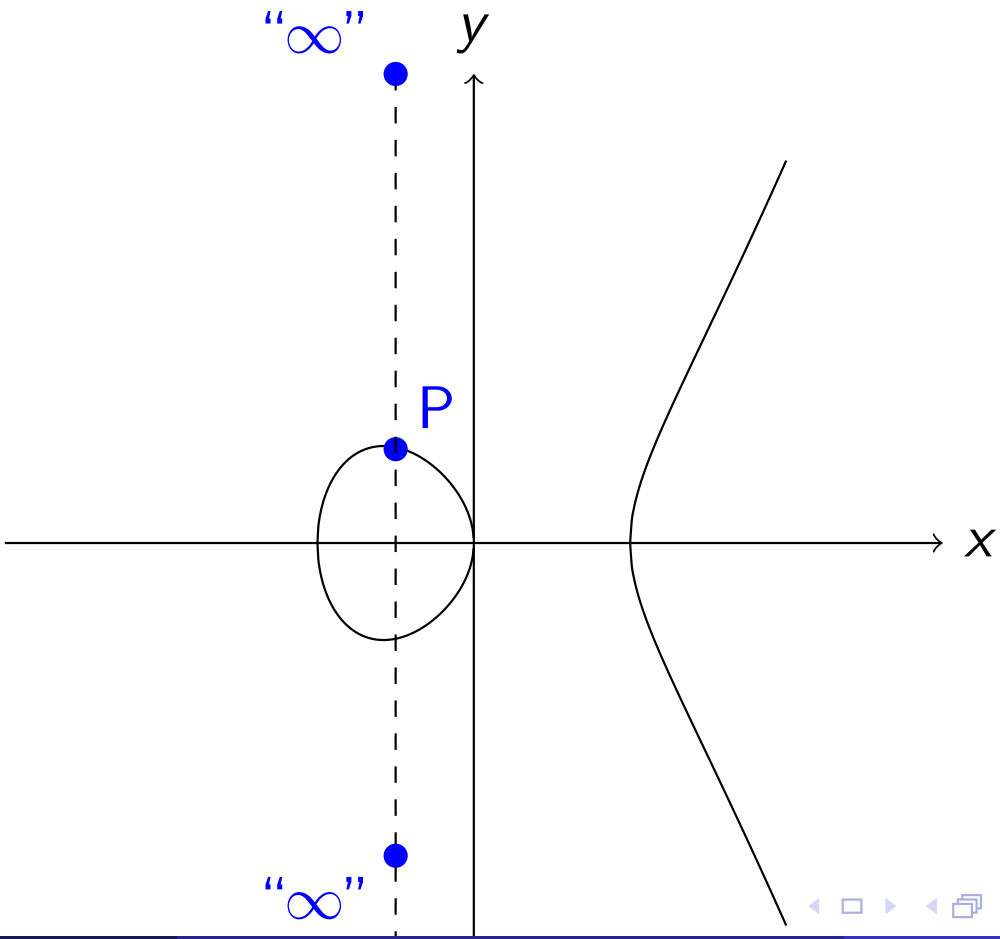
Point at Infinity

- **Point at Infinity**: In the projective plane, all lines intersect, so the vertical line through any point P on the curve intersects the curve at a "point at infinity". This point serves as the identity element of the group.



Point at Infinity

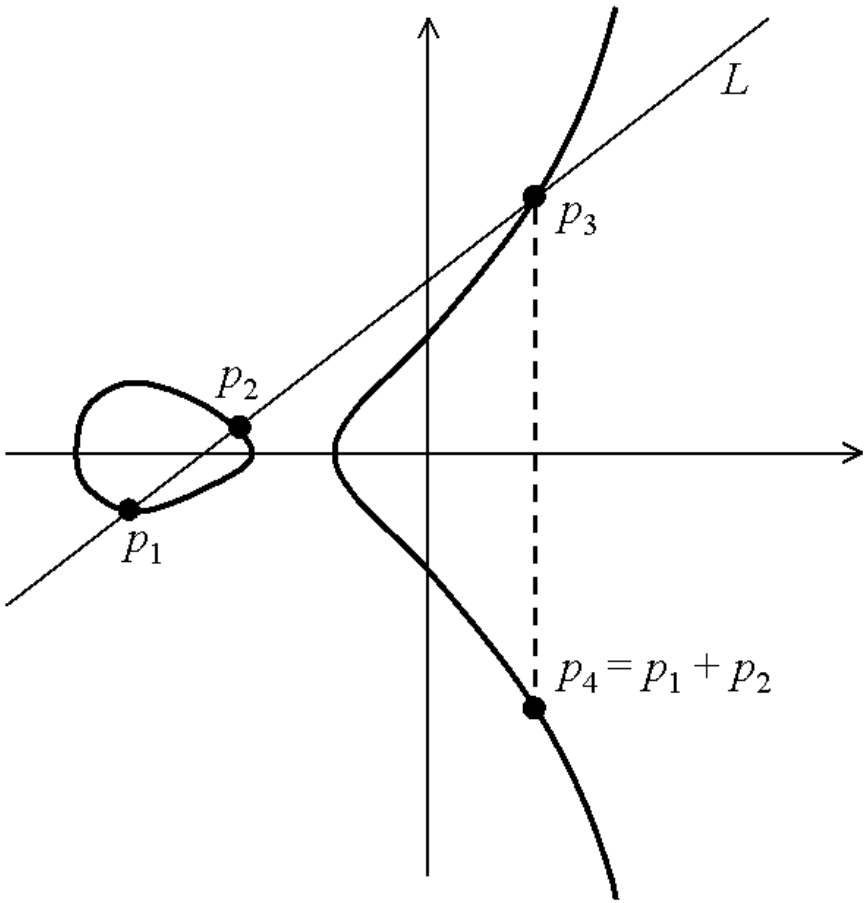
- **Point at Infinity**: In the projective plane, all lines intersect, so the vertical line through any point P on the curve intersects the curve at a "point at infinity". This point serves as the identity element of the group.



The Group Law on Elliptic Curves

- Elliptic curves form a group under a geometric operation called point addition.
- Given two points P and Q on the curve, the line passing through P and Q intersects the curve at a third point R.
- The reflection of R in the x-axis is defined as the sum of P and Q, denoted as $P + Q$.
- This point addition operation is associative, meaning $(P + Q) + R = P + (Q + R)$ for any points P, Q, and R on the curve.
- The identity element in this group is the point at infinity, denoted as $O = \infty$. The sum of O with any point P is P itself, i.e., $P + O = P$.
- Every point P on the curve has an inverse -P, which is the reflection of P in the x-axis. The sum of P and its inverse is O, i.e., $P + (-P) = O$.

Dynamics of the elliptic curves



Rational map of $E(\mathbb{R}) : y^2 = x^3 + ax + b$

Rational map of $E(\mathbb{R}) : y^2 = x^3 + ax + b$

$$E(\mathbb{R}) \longrightarrow \mathbb{P}^1(\mathbb{R}), (x, y) \longmapsto x$$

Rational map of $E(\mathbb{R}) : y^2 = x^3 + ax + b$

$$E(\mathbb{R}) \longrightarrow \mathbb{P}^1(\mathbb{R}), (x, y) \longmapsto x$$

$$\begin{array}{ccc} E(\mathbb{R}) & \xrightarrow{[2]} & E(\mathbb{R}) \\ \downarrow x & & \downarrow x \\ \mathbb{P}^1(\mathbb{R}) & \xrightarrow{\phi_{E,2}} & \mathbb{P}^1(\mathbb{R}) \end{array}$$

Rational map of $E(\mathbb{R}) : y^2 = x^3 + ax + b$

$$E(\mathbb{R}) \longrightarrow \mathbb{P}^1(\mathbb{R}), (x, y) \longmapsto x \qquad \begin{array}{ccc} E(\mathbb{R}) & \xrightarrow{[2]} & E(\mathbb{R}) \\ \downarrow x & & \downarrow x \\ \mathbb{P}^1(\mathbb{R}) & \xrightarrow{\phi_{E,2}} & \mathbb{P}^1(\mathbb{R}) \end{array}$$

$$\phi_{E,2}(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$$

$\phi_{E,2}(x)$ is called a **Lattès map**

Torsion points of $E(\mathbb{Q}) : y^2 = x^3 + ax + b$

Definition

Let $E(\mathbb{Q})$ be an elliptic curve. $P = (x_P, y_P) \in E(\mathbb{Q})$ is a **torsion point** if (x_P, y_P) has finite order under addition.

Torsion points of $E(\mathbb{Q}) : y^2 = x^3 + ax + b$

Definition

Let $E(\mathbb{Q})$ be an elliptic curve. $P = (x_P, y_P) \in E(\mathbb{Q})$ is a **torsion point** if (x_P, y_P) has finite order under addition.

It is equivalent to

"x has finite orbit under $\phi_{E,2}(x) = \dfrac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$."

Torsion points of $E(\mathbb{Q}) : y^2 = x^3 + ax + b$

Definition

Let $E(\mathbb{Q})$ be an elliptic curve. $P = (x_P, y_P) \in E(\mathbb{Q})$ is a **torsion point** if (x_P, y_P) has finite order under addition.

It is equivalent to

"x has finite orbit under $\phi_{E,2}(x) = \dfrac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$."

Remark The set of torsion points of an elliptic curve forms a group called "torsion subgroup".

Some results on torsion subgroups

- **Mordell-Weil Theorem(1922)** $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, where $T = E_{tors}(\mathbb{Q})$ is a finite group.

Some results on torsion subgroups

- **Mordell-Weil Theorem(1922)** $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, where $T = E_{tors}(\mathbb{Q})$ is a finite group.
- **Mazur Theorem(1978)** T is isomorphic to one of the following:
  $\mathbb{Z}_n$ with $1 \leq 10$ or $n = 12$,
  $\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$ with $1 \leq n \leq 4$.

Some results on torsion subgroups

- **Mordell-Weil Theorem(1922)** $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, where $T = E_{tors}(\mathbb{Q})$ is a finite group.
- **Mazur Theorem(1978)** T is isomorphic to one of the following:
  $\mathbb{Z}_n$ with $1 \leq 10$ or $n = 12$,
  $\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$ with $1 \leq n \leq 4$.
- **Merel Theorem(1994)** For every integer $d \geq 1$ there is a constant $N(d)$ such that for all number fields $K/\mathbb{Q}$ of degree at most d and all elliptic curves $E(K)$,

$$|E_{tors}(K)| \leq N(d).$$

References for Studying Elliptic Curves

Books:

1. Silverman, J. H., *The Arithmetic of Elliptic Curves*. Springer, 2009. - A comprehensive introduction to the arithmetic and geometry of elliptic curves.
2. Washington, L. C., *Elliptic Curves: Number Theory and Cryptography*. CRC Press, 2008. - Covers elliptic curves from a number-theoretic and cryptographic perspective.
3. Cassels, J. W. S., *Lectures on Elliptic Curves*. Cambridge University Press, 1991. - Provides an introduction to the theory of elliptic curves.
4. Silverman, J. H., and Tate, J., *Rational Points on Elliptic Curves*. Springer, 1992. - Focuses on the arithmetic of rational points on elliptic curves.

References for Studying Elliptic Curves (Continued)

Online Resources:

1. SageMath Documentation on Elliptic and Hyperelliptic Curves
   - `https://doc.sagemath.org/html/en/reference/arithmetic_curves/index.html`
   - `https://doc.sagemath.org/pdf/en/reference/arithmetic_curves/arithmetic_curves.pdf`