Algebraic Geometry: Elliptic Curves and 2 Theorems

Chris Zhu

Mentor: Chun Hong Lo
MIT PRIMES

December 7, 2018
Rational Parametrization

- Plane curves: finding rational points on such curves
Rational Parametrization

- Plane curves: finding rational points on such curves
- Motivation: studying structures involving the rationals is generally nicer
Rational Parametrization

- Plane curves: finding rational points on such curves
- Motivation: studying structures involving the rationals is generally nicer
- Linear and quadratic equations: formulas exist!
Rational Parametrization

- Plane curves: finding rational points on such curves
- Motivation: studying structures involving the rationals is generally nicer
- Linear and quadratic equations: formulas exist!
Rational Parametrization (cont’d)

- Rational $x$-coordinates give rational $y$-coordinates on a line

\[(m, 0)\]

Extending projection to degree 3:
Rational Parametrization (cont’d)

- Rational $x$-coordinates give rational $y$-coordinates on a line
- $\left( \frac{m}{n}, 0 \right)$ is projected onto the circle as $\left( \frac{2mn}{m^2 + n^2}, \frac{n^2 - m^2}{n^2 + m^2} \right)$
Rational Parametrization (cont’d)

- Rational $x$-coordinates give rational $y$-coordinates on a line
- $\left(\frac{m}{n}, 0\right)$ is projected onto the circle as $\left(\frac{2mn}{m^2 + n^2}, \frac{n^2 - m^2}{n^2 + m^2}\right)$
- Extending projection to degree 3:
Connecting 2 points on an elliptic curve is similar to standard addition.
Connecting 2 points on an elliptic curve is similar to standard addition.

- We are very familiar with structures like \( \mathbb{Z} \) which use addition.
Connecting 2 points on an elliptic curve is similar to standard addition.

- We are very familiar with structures like $\mathbb{Z}$ which use addition.
- To understand rational points on elliptic curves, can we give them similar structure?
Connecting 2 points on an elliptic curve is similar to standard addition.

- We are very familiar with structures like $\mathbb{Z}$ which use addition.
- To understand rational points on elliptic curves, can we give them similar structure?

If we can assign such a structure, finding rational points is a lot simpler:

**Example.**

$\mathbb{Z}$ is generated by $-1$ or $1$; $\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$ is generated by anything but 0.

Instead of looking for all rational points, we can try to find a generating set.
What is a Group?

A group \((G, \circ)\) is a set \(G\) with a law of composition \((a, b) \mapsto a \circ b\) satisfying the following:

- **Associativity:** \((a \circ b) \circ c = a \circ (b \circ c)\)
- **Identity element:** \(\exists e \in G\) such that \(a \circ e = e \circ a = a\)
- **Inverse element:** for \(a \in G\), \(\exists a^{-1} \in G\) such that \(a \circ a^{-1} = a^{-1} \circ a = e\)
What is a Group?

A group \((G, \circ)\) is a set \(G\) with a law of composition \((a, b) \mapsto a \circ b\) satisfying the following:

- **Associativity:** \((a \circ b) \circ c = a \circ (b \circ c)\)
- **Identity element:** \(\exists e \in G\) such that \(a \circ e = e \circ a = a\)
- **Inverse element:** for \(a \in G\), \(\exists a^{-1} \in G\) such that \(a \circ a^{-1} = a^{-1} \circ a = e\)

**Example.**

\((\mathbb{Z}, +)\) and \((\mathbb{Z}_n, +)\) are groups, as well as \((\text{GL}_2(\mathbb{R}), \times)\) where

\[
\text{GL}_2(\mathbb{R}) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } A \text{ is invertible} \right\}.
\]
If we tweak the "addition" of points mentioned before, we get a group structure for the rational points on an elliptic curve!
If we tweak the "addition" of points mentioned before, we get a group structure for the rational points on an elliptic curve!

But, what about...
If we tweak the "addition" of points mentioned before, we get a group structure for the rational points on an elliptic curve!

But, what about...
- Identity?
If we tweak the "addition" of points mentioned before, we get a group structure for the rational points on an elliptic curve!

But, what about...

- Identity?
- Tangent lines?
Definition.

(Projective space) Define the equivalence relation $\sim$ by $(x_0, x_1, ..., x_n) \sim (y_0, y_1, ..., y_n)$ if $\exists \lambda \in k$ such that $y_i = \lambda x_i$. Then, we define real projective $n$-space as

$$\mathbb{P}^n = \frac{\mathbb{R}^{n+1} - \{0\}}{\sim}.$$
Definition.

(Projecive space) Define the equivalence relation \( \sim \) by \((x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n) \) if \( \exists \lambda \in k \) such that \( y_i = \lambda x_i \). Then, we define real projective \( n \)-space as

\[
P^n = \frac{\mathbb{R}^{n+1} - \{0\}}{\sim}.
\]

Why does this definition help us?
Definition.

(Projective space) Define the equivalence relation \( \sim \) by \((x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)\) if \( \exists \lambda \in k \) such that \( y_i = \lambda x_i \). Then, we define real projective \( n \)-space as

\[
P^n = \frac{\mathbb{R}^{n+1} - \{0\}}{\sim}.
\]

Why does this definition help us?

- Added "points at infinity" — \( \mathbb{P}^1 \) can be seen as \( \mathbb{R}^1 \cup \infty \) and \( \mathbb{P}^2 \) as \( \mathbb{R}^2 \cup \mathbb{P}^1 \).
Solution: Projective Geometry

Definition.

(Projective space) Define the equivalence relation \(\sim\) by \((x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)\) if \(\exists \lambda \in k\) such that \(y_i = \lambda x_i\). Then, we define real projective \(n\)-space as

\[
P^n = \frac{\mathbb{R}^{n+1} - \{0\}}{\sim}.
\]

Why does this definition help us?

- Added ”points at infinity” — \(P^1\) can be seen as \(\mathbb{R}^1 \cup \infty\) and \(P^2\) as \(\mathbb{R}^2 \cup P^1\).
- Bézout’s theorem guarantees 3 intersection points.
Now we can answer our questions from before about the group structure of the rational points: point at infinity on the curve, denoted $O$, is the identity.
Tangent lines do have “3” intersections:
The group of rational points on an elliptic curve $E$ is denoted as $E(\mathbb{Q})$.

**Definition.**

An element $P$ of a group $G$ is said to have **order** $m$ if $m$ is the minimal natural number satisfying $mP = P \circ P \circ \ldots \circ P$ ($m$ times) = $e$. If no such $m$ exists, $P$ has **infinite order**.
The group of rational points on an elliptic curve $E$ is denoted as $E(\mathbb{Q})$.

**Definition.**

An element $P$ of a group $G$ is said to have order $m$ if $m$ is the minimal natural number satisfying $mP = P \circ P \circ \ldots \circ P$ ($m$ times) $= e$. If no such $m$ exists, $P$ has infinite order.

**Example.**

The order of every element in $(\mathbb{Z}/8\mathbb{Z})^\times$ is 2.
The group of rational points on an elliptic curve $E$ is denoted as $E(\mathbb{Q})$.

**Definition.**

An element $P$ of a group $G$ is said to have order $m$ if $m$ is the minimal natural number satisfying $mP = P \circ P \circ \ldots \circ P$ ($m$ times) $= e$. If no such $m$ exists, $P$ has infinite order.

**Example.**

The order of every element in $(\mathbb{Z}/8\mathbb{Z})^\times$ is 2.

**Definition.**

The torsion subgroup of a group $G$ is the set of all elements of $G$ with finite order.

- Can we determine $E(\mathbb{Q})_{\text{tors}}$?
Definition.

A set $S \subset G$ for a group $G$ is a **generating set** if all elements can be written as combinations of elements in $S$ under the group operation.
Definition.

A set $S \subseteq G$ for a group $G$ is a generating set if all elements can be written as combinations of elements in $S$ under the group operation.

Example.

The rationals are generated by the (infinite) set of unit fractions $\frac{1}{n}$ with $n \in \mathbb{N}$. 

Can we determine the generating set for $E(\mathbb{Q})$, and is it finite or infinite?
Definition.

A set $S \subset G$ for a group $G$ is a generating set if all elements can be written as combinations of elements in $S$ under the group operation.

Example.

The rationals are generated by the (infinite) set of unit fractions $\frac{1}{n}$ with $n \in \mathbb{N}$.

- Can we determine the generating set for $E(\mathbb{Q})$, and is it finite or infinite?
The Nagell-Lutz Theorem

Theorem.
Let \( y^2 = x^3 + ax^2 + bx + x \) be a non-singular elliptic curve with integral coefficients, and let \( D \) be the discriminant of the polynomial, 
\[
D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.
\]
Any point \((x, y)\) of finite order must have \(x, y \in \mathbb{Z}\) and \(y|D\).
The Nagell-Lutz Theorem

**Theorem.**

Let \( y^2 = x^3 + ax^2 + bx + x \) be a non-singular elliptic curve with integral coefficients, and let \( D \) be the discriminant of the polynomial, \( D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \). Any point \((x, y)\) of finite order must have \( x, y \in \mathbb{Z} \) and \( y | D \).

**Remark.**

There is a stronger form of the theorem which includes \( y^2 | D \).
The Nagell-Lutz Theorem

**Theorem.**

Let $y^2 = x^3 + ax^2 + bx + x$ be a non-singular elliptic curve with integral coefficients, and let $D$ be the discriminant of the polynomial, $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Any point $(x, y)$ of finite order must have $x, y \in \mathbb{Z}$ and $y|D$.

**Remark.**

There is a stronger form of the theorem which includes $y^2|D$.

**Example.**

The points $\{O, (1, 1), (0, 0), (1, -1)\}$ are the points of finite order on $y^2 = x^3 - x^2 + x$. 
Example.

Given a prime $p$, $E(\mathbb{Q})_{\text{tors}}$ for $y^2 = x^3 + px$ is always $\{O, (0, 0)\}$. 
Example.

Given a prime $p$, $E(\mathbb{Q})_{\text{tors}}$ for $y^2 = x^3 + px$ is always $\{O, (0, 0)\}$. 
Mordell’s Theorem

**Theorem.**

(Mordell’s Theorem) Let $E$ be a non-singular elliptic curve with a rational point of order 2. Then $E(\mathbb{Q})$ is a finitely generated abelian group.

Any finitely generated abelian group $G$ can be written as $\mathbb{Z}^r \oplus G_{\text{tors}}$, where $r$ is called the rank. The rank can be computed by solving some Diophantine equations.
(Mordell’s Theorem) Let $E$ be a non-singular elliptic curve with a rational point of order 2. Then $E(\mathbb{Q})$ is a finitely generated abelian group.

Any finitely generated abelian group $G$ can be written as $\mathbb{Z}^r \oplus G_{\text{tors}}$, where $r$ is called the rank. The rank can be computed by solving some Diophantine equations.

Example.

Given a prime $p$, the rank of $y^2 = x^3 + px$ is either 0, 1, or 2.
Theorem. (Mazur’s Theorem) Let $E$ be a non-singular cubic curve with rational coefficients, and suppose $P \in E(\mathbb{Q})$ has order $m$. Then either $1 \leq m \leq 10$ or $m = 12$. The only possible torsion subgroups are isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for $1 \leq N \leq 10$ or $N = 12$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ for $1 \leq N \leq 4$. 

Genus-degree formula: $g = \left(\frac{d-1}{2}\right)\left(\frac{d-2}{2}\right)$ for curves in $\mathbb{P}^2$. 

Theorem. (Falting’s Theorem) A curve of genus greater than 1 has only finitely many rational points.
Theorem.

(Mazur's Theorem) Let $E$ be a non-singular cubic curve with rational coefficients, and suppose $P \in E(\mathbb{Q})$ has order $m$. Then either $1 \leq m \leq 10$ or $m = 12$. The only possible torsion subgroups are isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for $1 \leq N \leq 10$ or $N = 12$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ for $1 \leq N \leq 4$.

Genus-degree formula: $g = \frac{(d - 1)(d - 2)}{2}$ for curves in $\mathbb{P}^2$.

Theorem.

(Falting's Theorem) A curve of genus greater than 1 has only finitely many rational points.
I would like to thank the following:

- My mentor, Chun Hong Lo
- My parents
- The PRIMES program
Acknowledgements

I would like to thank the following:

- My mentor, Chun Hong Lo
Acknowledgements

I would like to thank the following:

- My mentor, Chun Hong Lo
- My parents
Acknowledgements

I would like to thank the following:

- My mentor, Chun Hong Lo
- My parents
- The PRIMES program