Mordell-Weil Theorem

Lukáš Perůtka

Faculty of Mathematics and Physics
Charles University in Prague

Spring school of Algebra
March 24-28, 2010

Content

The Group of Rational Points

- The set of all rational points on a non-singular elliptic curve forms a group.

The Group of Rational Points

- The set of all rational points on a non-singular elliptic curve forms a group.
- The group is Abelian.

The Group of Rational Points

- The set of all rational points on a non-singular elliptic curve forms a group.
- The group is Abelian.
- We will show that the group of rational points on a non-singular elliptic curve is finitely generated:

$$\Gamma \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}}$$

The Group of Rational Points

- The set of all rational points on a non-singular elliptic curve forms a group.
- The group is Abelian.
- We will show that the group of rational points on a non-singular elliptic curve is finitely generated:

$$\Gamma \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}}$$

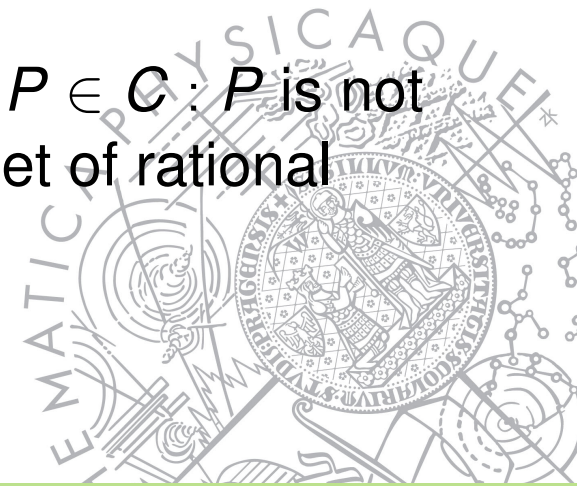
- Singular case?

The Group of Rational Points

- The set of all rational points on a non-singular elliptic curve forms a group.
- The group is Abelian.
- We will show that the group of rational points on a non-singular elliptic curve is finitely generated:

$$\Gamma \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}}$$

- For a singular curve C we define a set $C_{ns} = \{P \in C : P \text{ is not a singular point }\}$. C_{ns} forms a group and the set of rational points $C_{sn}(\mathbb{Q})$ is also a group.



The Group of Rational Points

- The set of all rational points on a non-singular elliptic curve forms a group.
- The group is Abelian.
- We will show that the group of rational points on a non-singular elliptic curve is finitely generated:

$$\Gamma \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}}$$

- For a singular curve C we define a set $C_{ns} = \{P \in C : P \text{ is not a singular point }\}$. C_{ns} forms a group and the set of rational points $C_{sn}(\mathbb{Q})$ is also a group.
- It is not difficult to show that the group $C_{sn}(\mathbb{Q})$ is not finitely generated.

Height

We begin by defining the height of a rational number.

Definition

Let $x = \frac{m}{n}$ be a rational number written in lowest terms. Then we define the *height*

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}.$$

Height

We begin by defining the height of a rational number.

Definition

Let $x = \frac{m}{n}$ be a rational number written in lowest terms. Then we define the *height*

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}.$$

Definition

Let $P = (x, y)$ be a rational point on a elliptic curve C. Then we define the *height* of P

$$H(P) = H(x).$$

Basic facts about Height

- The set of all rational numbers whose height is less than some fixed number is finite.

Basic facts about Height

- The set of all rational numbers whose height is less than some fixed number is finite.
- The Height has some multiplicative behaviour.

Basic facts about Height

- The set of all rational numbers whose height is less than some fixed number is finite.
- The Height has some multiplicative behaviour.
- We have rather something that behaves additively so we define

$$h(P) = \log H(P).$$

Basic facts about Height

- The set of all rational numbers whose height is less than some fixed number is finite.
- The Height has some multiplicative behaviour.
- We have rather something that behaves additively so we define

$$h(P) = \log H(P).$$

- Let $\mathcal{O}$ be a point at infinity. We define $H(\mathcal{O}) = 1$, $h(\mathcal{O}) = 0$.

Supporting Lemmas

Let $y^2 = x^3 + ax^2 + bx + c$ be a non-singular curve C with $a, b, c \in \mathbb{Z}$.

Lemma (1)

For every real number M, the set

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\}$$

is finite.

Supporting Lemmas

Let $y^2 = x^3 + ax^2 + bx + c$ be a non-singular curve C with $a, b, c \in \mathbb{Z}$.

Lemma (1)

For every real number M, the set

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\}$$

is finite.

Lemma (2)

Let P_0 be a fixed rational point on C. There is a constant κ_0, depending on P_0 and on a, b, c, so that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \text{for all} \quad P \in C(\mathbb{Q}).$$

Supporting Lemmas

Lemma (3)

There is a constant κ, depending on a, b, c, so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all} \quad P \in C(\mathbb{Q}).$$

Supporting Lemmas

Lemma (3)

There is a constant κ, depending on a, b, c, so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all} \quad P \in C(\mathbb{Q}).$$

Lemma (4)

The index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite.

Mordell-Weil Theorem

Theorem (Mordell-Weil Theorem)

Let C be a non-singular cubic curve given by an equation

$$C : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Z}$. Then the group of rational points $\Gamma = C(\mathbb{Q})$ is a finitely generated abelian group.

Idea of Proof

- Lemma 4 gives us something finite.

Idea of Proof

- Lemma 4 gives us something finite.
- So we start with this lemma.

Idea of Proof

- Lemma 4 gives us something finite.
- So we start with this lemma.
- If we will be able to express every point from Γ as a sum of the representatives for the cosets of 2Γ and some others points about which we know that they have some limited height.

Idea of Proof

- Lemma 4 gives us something finite.
- So we start with this lemma.
- If we will be able to express every point from Γ as a sum of the representatives for the cosets of 2Γ and some others points about which we know that they have some limited height.
- Then according to Lemma 1 we are finished.

Proof of Mordell-Weil Theorem

- From Lemma 4 we know that there are only finitely many cosets of 2Γ in Γ.

Proof of Mordell-Weil Theorem

- From Lemma 4 we know that there are only finitely many cosets of 2Γ in Γ.
- Let $Q_1, \ldots, Q_n$ be representatives for the cosets, where $n \in \mathbb{N}$.

Proof of Mordell-Weil Theorem

- From Lemma 4 we know that there are only finitely many cosets of 2Γ in Γ.
- Let $Q_1, \ldots, Q_n$ be representatives for the cosets, where $n \in \mathbb{N}$.
- So take $P \in \Gamma$. Then there is an index i_1 such that

$$P - Q_{i_1} \in 2\Gamma.$$

Proof of Mordell-Weil Theorem

- From Lemma 4 we know that there are only finitely many cosets of 2Γ in Γ.
- Let $Q_1, \ldots, Q_n$ be representatives for the cosets, where $n \in \mathbb{N}$.
- So take $P \in \Gamma$. Then there is an index i_1 such that

$$P - Q_{i_1} \in 2\Gamma.$$

- In other words there exists $P_1 \in \Gamma$ such that

$$P - Q_{i_1} = 2P_1.$$

Proof of Mordell-Weil Theorem

- From Lemma 4 we know that there are only finitely many cosets of 2Γ in Γ.
- Let $Q_1, \ldots, Q_n$ be representatives for the cosets, where $n \in \mathbb{N}$.
- So take $P \in \Gamma$. Then there is an index i_1 such that

$$P - Q_{i_1} \in 2\Gamma.$$

- In other words there exists $P_1 \in \Gamma$ such that

$$P - Q_{i_1} = 2P_1.$$

- We can do the same thing with P_1, P_2, etc...

Proof of Mordell-Weil Theorem

- We get:

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

Proof of Mordell-Weil Theorem

- We get:

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

- So we can express P as

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_{m-1}} + 2^m P_m.$$

Proof of Mordell-Weil Theorem

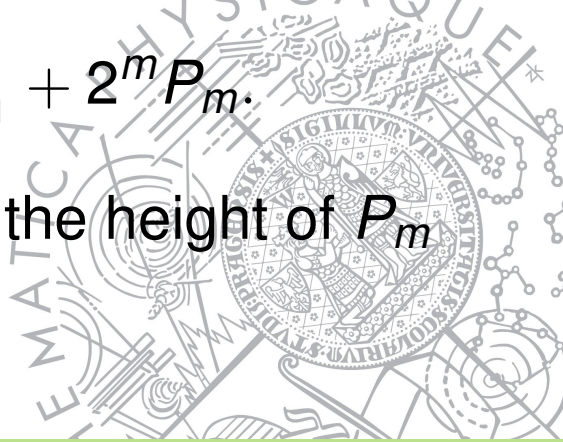
- We get:

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

- So we can express P as

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_{m-1}} + 2^m P_m.$$

- Now we want to show that for m large enough, the height of P_m is less than a certain fixed bound.



Proof of Mordell-Weil Theorem

- If we fix Q_i, we get a constant κ_i from Lemma 2 such that

$$h(P - Q_i) \leq 2h(P) + \kappa_i \text{ for all } P \in \Gamma.$$

Proof of Mordell-Weil Theorem

- If we fix Q_i, we get a constant κ_i from Lemma 2 such that

$$h(P - Q_i) \leq 2h(P) + \kappa_i \text{ for all } P \in \Gamma.$$

- So let κ' be the largest of $\{\kappa_i; 1 \leq i \leq n\}$.

Proof of Mordell-Weil Theorem

- If we fix Q_i, we get a constant κ_i from Lemma 2 such that

$$h(P - Q_i) \leq 2h(P) + \kappa_i \text{ for all } P \in \Gamma.$$

- So let κ' be the largest of $\{\kappa_i; 1 \leq i \leq n\}$.
- If we use Lemma 3, we get

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa + \kappa'.$$

Proof of Mordell-Weil Theorem

- If we fix Q_i, we get a constant κ_i from Lemma 2 such that

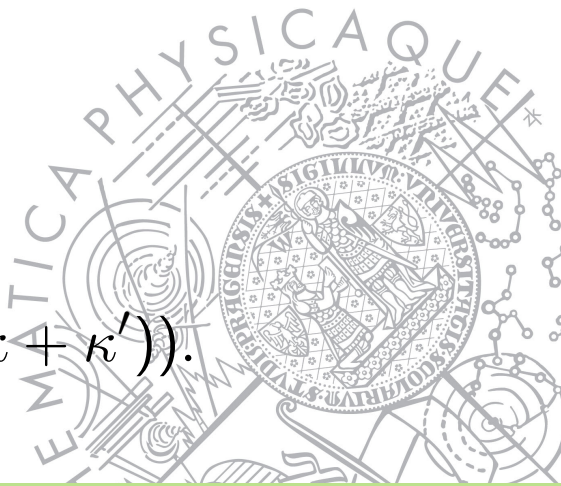
$$h(P - Q_i) \leq 2h(P) + \kappa_i \text{ for all } P \in \Gamma.$$

- So let κ' be the largest of $\{\kappa_i; 1 \leq i \leq n\}$.
- If we use Lemma 3, we get

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa + \kappa'.$$

- We rewrite this as

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa + \kappa'}{4} = \\ &= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa + \kappa')). \end{aligned}$$



Proof of Mordell-Weil Theorem

- We have a sequence of points $P, P_1, P_2, \ldots$

Proof of Mordell-Weil Theorem

- We have a sequence of points $P, P_1, P_2, \ldots$
- If $h(P_{j-1}) \geq \kappa + \kappa'$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1}).$$

Proof of Mordell-Weil Theorem

- We have a sequence of points $P, P_1, P_2, \ldots$
- If $h(P_{j-1}) \geq \kappa + \kappa'$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1}).$$

- Because $\left(\frac{3}{4}\right)^k \searrow 0$ for $k \to \infty$, there is an index m such that $h(P_m) \leq \kappa + \kappa'$.

Proof of Mordell-Weil Theorem

- We have a sequence of points $P, P_1, P_2, \ldots$
- If $h(P_{j-1}) \geq \kappa + \kappa'$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1}).$$

- Because $\left(\frac{3}{4}\right)^k \searrow 0$ for $k \to \infty$, there is an index m such that $h(P_m) \leq \kappa + \kappa'$.
- We have shown that every point $P \in \Gamma$ can be written in the form

$$P = a_1 Q_1 + a_2 Q_2 + a_3 Q_3 + \ldots + a_n Q_n + 2^m R,$$

where $a_i \in \mathbb{Z}$ and $h(R) \leq \kappa + \kappa'$.

Proof of Mordell-Weil Theorem

So the set

$$\{Q_1, Q_2, Q_3, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa + \kappa'\}$$

generates Γ. From Lemma 1 and Lemma 4, this set is finite.

Rank

Definition

Let

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r\times} \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}}$$

be the group of rational points on the elliptic curve, then integer r is called the *rank* of Γ.

Torsion subgroup

The group Γ is finite if and only if $r = 0$.

Torsion subgroup

The group Γ is finite if and only if $r = 0$.

Theorem (Mazur)

The torsion subgroup of Γ *is isomorphic to exactly one of the following groups:*

$$\mathbb{Z}_n \;\; 1 \leq n \leq 10 \;\; \textit{or} \;\; n = 12,$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \;\; 1 \leq n \leq 4.$$

Torsion subgroup

The group Γ is finite if and only if $r = 0$.

Theorem (Mazur)

The torsion subgroup of Γ *is isomorphic to exactly one of the following groups:*

$$\mathbb{Z}_n \;\; 1 \leq n \leq 10 \;\; \textit{or} \;\; n = 12,$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \;\; 1 \leq n \leq 4.$$

So we know exactly how the torsion subgroup looks like.

Possible values of Rank

- There isn’t any algorithm that could compute a rank of arbitrary curve.

Possible values of Rank

- There isn’t any algorithm that could compute a rank of arbitrary curve.
- We suppose that there do not exist any limit for a rank.

Possible values of Rank

- There isn't any algorithm that could compute a rank of arbitrary curve.
- We suppose that there do not exist any limit for a rank.
- Elkies (2009) found a curve with the rank 19 (exactly).

Possible values of Rank

- There isn't any algorithm that could compute a rank of arbitrary curve.
- We suppose that there do not exist any limit for a rank.
- Elkies (2009) found a curve with the rank 19 (exactly).
- Elkies (2006) found a curve with the rank at least 28.

Q&A

Q&A

Thank you for your attention.