Mordell's Theorem

Carl Wolter and Annika Weidmann

24. October 2023

Why is Mordell's Theorem interesting?

In this talk we will outline a proof for the following theorem due to Louis Mordell (see the end of Section 1.2 in [1]):

Theorem 1 (Mordell's Theorem)**.** *If a non-singular rational plane cubic curve has a rational point, then the group of rational points is finitely generated.*

Louis Mordell first proved it in [6] in 1922. He was born in Philadelphia, Pennsylvania, on 28 January 1888 as the son of Phineas Mordell, who had immigrated from Lithuania and later became a reknown Hebrew scholar. In the exam for a scholarship at the university of Cambridge Louis Mordell excelled and outperformed all other candidates and so he persuade his studies there. He later was professor at Manchester University and Cambridge and also obtained the British citizenship [7]. Besides the above theorem another important contribution of Mordell was the proof of Ramanujans conjecture about the τ-function by using modular forms [8]. Mordell died in 1972 in Cambridge [7].

The above theorem was generalized by Weil to what is now known as the Mordell-Weil Theorem, which states that for an abelian variety A over a number field K (i.e. $K/\mathbb{Q}$ is finite) the group $A(K)$ of K-rational points of A is a finitely-generated group. Néron even further generalized this theorem to fields which are a finite extension over their prime field of arbitrary characteristics [9].

Now back to the topic of this talk and the above theorem. The usefulness and beauty of Mordell's theorem becomes apparent, when we reformulate it in more concrete and geometric terms. It says that we only need finitely many (rational) points on the curve and the geometrically defined group law to write any rational point on the curve. So if our goal was to understand the set of rational points on an elliptic curve, we could probably declare victory (at least for the non-singular plane cubic case) – once we have proven Mordell's theorem. So let's get started.

The Proof

Since the proof of Mordell's theorem is somewhat long, following Chapter 3 in [1], we have broken it down into several parts. The second part will be concerned with the Descent Theorem and finish up the proof of Mordell's Theorem. The first part will establish that a key assumption for the Descent Theorem actually holds for our curve.

1 Part I: $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is Finite

In this part we will present the proof of the following Lemma which is Lemma 3.4 in [1].

Lemma 1. *The index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite.*

First, we will call $C(\mathbb{Q}) =: \Gamma$ for convenience. Then what we want to prove becomes

$$(\Gamma : 2\Gamma) < +\infty \ .$$

Unfortunately, if we want to avoid using too much algebraic number theory we cannot prove this in all its generality. Instead we will have to assume that our curve

$$y^2 = f(x) = x^3 + ax^2 + bx + c \quad \text{for } a, b, c \in \mathbb{Z}$$

has at least one rational root x_0. We know from the previous talk on Points of finite order that x_0 then is a rational point of order two (see Theorem 1.1 in [2]). This will later be of importance. Now it is more interesting to observe that if x_0 is the root of a quadratic polynomial with integer coefficients, then also x_0 must be an integer. Hence, we can replace $x \mapsto x - x_0$ and our equation will have the easier form

$$C: \ y^2 = f(x) = x^3 + ax^2 + bx \quad \text{for } a, b \in \mathbb{Z}.$$

Then our rational root is $T = (0, 0)$. Observe also that under this transformation we only translate the group of rational points by an integer and thus not change it relevantly.

The idea of the proof is to break down the map $P \mapsto 2P$ into two simpler maps. Then we will use the group theoretic fact that for maps $\phi; \Gamma \to B$ and $\psi : B \to \Gamma$ with $(\psi \circ \phi)(P) = 2P$ we have

$$(\Gamma : 2\Gamma) \leq (\Gamma : \psi(B)) \cdot (B : \phi(\Gamma)).$$

This fact can be proven quickly by thinking about the cosets and how to represent them in terms of each other. If we now moreover can show that the indexes on the right side are both finite, we would be done.

This is the technical way of how we will do this. But in the end we will see, that the moral reason for why $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite, is really the fact that modulo squares there are only finitely many possibilities for the x-coordinate of a rational point on the curve. But we will come back to that towards the end of this section.

1.1 Two Homomorphisms

We will now go about to define the ϕ and ψ that we were dreaming of above. Unfortunately, they will not be endomorphisms, meaning form our curve C to our curve C but we will have to make a little detour and visit another elliptic curve. We will call this other curve $\overline{C}$ and we will get it from C by

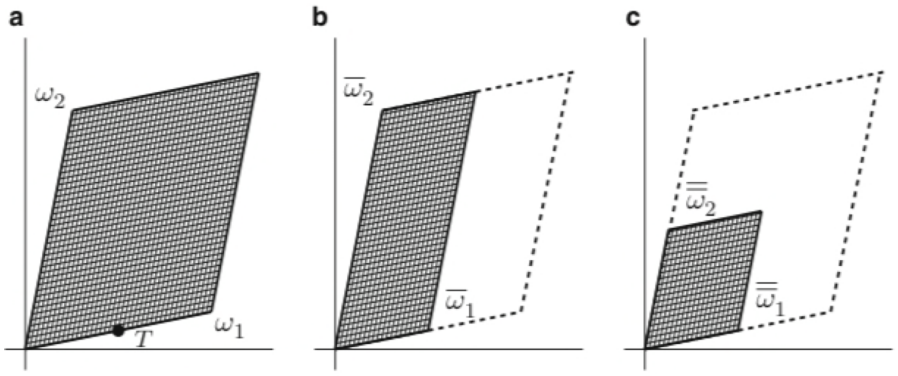
$$\overline{C}: \ y^2 = x^3 + \bar{a}x^2 + \bar{b}x \quad \bar{a} := -2a \text{ and } \bar{b} := a^2 - 4b \ .$$

Observe that it follows that

$$\begin{aligned}\overline{\overline{C}}:\ y^2 &= x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x \\ &= x^3 - 2\bar{a} + \bar{a}^2 - 4\bar{b} \\ &= x^3 + 4a + 4a^2 - 4(a^2 - 4b) \\ &= x^3 + 4a + 16b\end{aligned}$$

which we can transform by $x \mapsto 4x$, $y \mapsto 8y$ and then dividing by 64 in a purely rational way back to our original curve C. So also their groups of rational points are isomorphic. Thus, form now on we will identify $\overline{\overline{C}}$ with C.

In order to motivate the following definition, we would have to first internalize part of the content of Section 2.2 to of [1]. Cut short, this section says that to every elliptic curve there exists a complex meromorphic function $\wp$ called the *Weierstraß $\wp$-function* which has two periods in to linearly independent direction. We then can consider a so called *period parallelogram* onto which the function maps bijectively. The following image (which is figure 3.1 in [1]) is an example of such a period parallelogram.



This image also illustrates exactly what we want to do: We want to define a map ϕ from a curve C with a period parallelogram as in **a** to a curve $\overline{C}$ with period parallelogram as in **b** and another map ψ from $\overline{C}$ to a curve $\overline{\overline{C}} \approx C$ with a period parallelogram as in **c**. The parallelogram in **c** can clearly be seen to be the same as in **a** but for being scaled by $\frac{1}{2}$. Observe also that the point marked with T in the picture is a point of order two just as the point we are calling T. So it should not come very surprisingly that our point T of order two will play a special role in the definition we will make inside this Proposition, which is Proposition 3.7 in [1]:

Proposition 1. *Let C and $\overline{C}$ be elliptic curves given by the equations*

$$C:\ y^2 = f(x) = x^3 + ax^2 + bx \ \textit{and}\ \overline{C}:\ y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where

$$\bar{a} = -2a \ \textit{and}\ \bar{b} = a^2 - 4b\ .$$

Let $T = (0,0) \in C$.

(a) There is a homomorphism $\phi : C \to \overline{C}$ defined by

$$\phi((x,y)) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & \text{if } (x,y) \neq \mathcal{O},\ T \\ \overline{\mathcal{O}} & \text{if } (x,y) = \mathcal{O},\ T \end{cases}$$

(b) Analogously we get a map $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$. Using that $\overline{\overline{C}}$ is isomorphic to C via $(x,y) \mapsto (\frac{1}{4}x, \frac{1}{8}y$ we get that there is homomorphism $\psi : \overline{C} \to C$ defined by

$$\phi((\overline{x},\overline{y})) = \begin{cases} \left(\frac{\overline{y}^2}{\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{\overline{x}^2}\right) & \text{if } (\overline{x},\overline{y}) \neq \overline{\mathcal{O}},\ \overline{T} \\ \mathcal{O} & \text{if } (\overline{x},\overline{y}) = \overline{\mathcal{O}},\ \overline{T} \end{cases}$$

(c) The composition $\psi \circ \phi : C \to C$ is the multiplication by two map:

$$(\psi \circ \phi)(P) = 2P$$

The proof of this proposition is lengthy but consists mostly of elementary computations, therefore we will omit it. The interested reader can find it in section 3.4 of [1].

1.2 The Images of the homomorphisms and the Indexes

Instead we want to take a closer look at these two homomorphisms or to be more precise, we would like to study the image $\phi(\Gamma) \leq \overline{\Gamma}$. We observe the following three facts:

(i) $\overline{\mathcal{O}} \in \phi(\Gamma)$

(ii) $\overline{T} = (0,0) \in \phi(\Gamma) \iff \overline{b} = a^2 - 4b$

(iii) For $\overline{P} = (\overline{x},\overline{y})$ $\overline{\Gamma}$ with $\overline{x} \neq 0$ we have $\overline{P} \in \phi(\Gamma) \iff \overline{x}$ is the square of a rational number.

The first one holds by definition. For the second one observe that we immediately get $y = 0$ and thus using the factorization $x(x^2 + ax + b)$ of C, we see that x must be a root of the second factor. This it possible if and only if the determinant $a^2 - 4b$ of the second factor is a square. From left to right in the third fact is by definition. For the converse one has to check, that the two points one would expect should work (i.e. $x_{1,2} = \frac{1}{2}\left(\overline{x} - a \pm \frac{\overline{y}}{\sqrt{\overline{x}}}\right)$ and $y_{1,2} = \pm x_{1,2}\sqrt{\overline{x}}$) indeed lie on the curve C. This can be done by direct computation.

Knowing all of this we are now ready to prove the finiteness of the indexes of the images of the two homomorphism. Luckily, they are defined very analogously, so that it suffices to prove it for ψ and it also will follow for ϕ.

We will show that there exists an injective homomorphism from the quotient group $\Gamma/\psi(\Gamma)$ into a finite group. To that end consider the subgroup

$$\mathbb{Q}^{*2} = \{u^2 : u \in \mathbb{Q}\}$$

of the multiplicative group $\mathbb{Q}^*$ of the rational numbers. We define a map

$$\begin{aligned}\alpha(\mathcal{O}) &= 1 \mod \mathbb{Q}^{*2} \\ \alpha(T) &= b \mod \mathbb{Q}^{*2} \\ \alpha((x,y) &= x \mod \mathbb{Q}^{*2} \text{ if } x \neq 0.\end{aligned}$$

where b is the coefficient from our elliptic curve. Once we have proven that α is a homomorphism (which works exactly as expected, therefore, we will omit it) we can deduce from the above three properties (i), (ii) and (iii) that indeed $\ker \alpha = \text{im } \psi$ and so α induces an injective homomorphism $\Gamma/\psi(\Gamma) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$. But what about the promised finite subgroup? Let's state it as a proposition (see propostion 3.8. in [1].

Proposition 2. *Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing b, meaning $b = \prod_{i=1}^{t} p_i^{\nu_i}$. Then the image of α is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements*

$$\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t} : \epsilon_i \in \{0,1\}\}.$$

Hence, we get the bound $(\Gamma : \psi(\Gamma) \leq 2^{t+1}$. In particular, this index is finite.

To prove this proposition one can ask oneself the question, which x-coordinates can occur for points in Γ. In the last talk we saw a very useful lemma which is result number 2.2 in the notes to the talks on Heights [3] and can be found in section 3.2 in [1]. Namely, we can write $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ for $m, n, e \in \mathbb{Z}$. Using this and a divisibility argument, one can quickly prove the proposition.

Here we see, as mentioned in the beginning, that there are only finitely many possibilities for the x-coordinate of a rational point on C and dirctly . Now, as promised, we only need to use the group theoretic fact

$$(\Gamma : 2\Gamma) \leq (\Gamma : \psi(\overline{\Gamma})) \cdot (\overline{\Gamma} : \phi(\Gamma)) \ < +\infty$$

to conclude the finiteness of $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$.

2 Part II: The Descent Theorem

Theorem 2. *Let Γ be a commutative group, and suppose that there is a function*

$$h : \Gamma \to [0,\infty)$$

with the following three properties:

1. *For every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$*
2. *For every $P_0 \in \Gamma$ ther is a constant κ_0 so that*

$$h(P+P_0) \leq 2h(P) + \kappa_0 \text{ for all } P \in \Gamma$$

3. *There is a constant κ so that*

$$h(2P) \geq 4h(P) - \kappa \text{ for all } P \in \Gamma$$

Suppose further that

4. *The subgroup* 2Γ *has finite index in* Γ.

Then Γ *is finitely generated*

Proof. Because the index $(\Gamma : 2\Gamma)$ is finite, we define $(\Gamma : 2\Gamma) = n$. We now take a representative from each of the cosets of $\Gamma/2\Gamma$ and call them $Q_1, \ldots, Q_{\mathrm{n}}$, which means that for every $P \in \Gamma$ we have an index i_1 such that

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

since P is in one of the cosets, and so we can write:

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

for $P_1 \in \Gamma$. Repeating this, we get

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{\mathrm{m\text{-}1}} - Q_{i_m} &= 2P_m, \end{aligned}$$

where $Q_{i_2}, \ldots, Q_{i_{\mathrm{n}}} \in \{Q_1, \ldots, Q_{\mathrm{n}}\}$ and $P_1, \ldots, P_{\mathrm{m}} \in \Gamma$.
The idea now is that since $P_i \approx 2P_{\mathrm{i+1}}$, $h(P_{\mathrm{i+1}}) \approx \frac{h(P_i)}{4}$, so the points P, P_1, $P_2, \ldots$ have decreasing height, so we end up in a set of points of bounded height, which by a) is finite, completing the proof. We will now formalize these steps: We first substitute the first equation

$$P = 2P_1 + Q_{i_1}$$

into the second equation

$$P_1 = 2P_2 + Q_{i_2},$$

giving us

$$P = 4P_2 + 2Q_{i_2} + Q_{i_1}$$

and, by repeating this we get

$$P = 2^{\mathrm{m}}P_m + 2^{\mathrm{m\text{-}1}}Q_{i_m} + \ldots + 4Q_{i_3} + 2Q_{i_2} + Q_{i_1}, \ (*)$$

so P is in the subgroup generated by the Q_i's and P_m's.
We now show that we can choose m large enough, such that P_m will have height less than a fixed bound not depending on P. Then Γ will be generated by the set of points with height less than this bound and the Q_i, which together still form a finite set. Let P_j be in the set $\{P, P_1, P_2, \ldots\}$. We will now show that the height of P_j is considerably smaller than the height of $P_{j\text{-}1}$:
Using 2) with $P_0 = -Q_i$, we get that

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

where κ_i is some constant. We now denote as κ' the largest of all κ_i's, and for this we have that:

$$h(P - Q_i) \leq 2h(P) + \kappa' \text{ for all } P \in \Gamma \text{ and } 1 \leq \mathrm{i} \leq n,$$

which we can do, because there is only finitely many Q_i's. We now use 3):

$$\begin{aligned} 4h(P_j) &\leq h(2P_j) + \kappa \\ &= h(P_{j\text{-}1} - Q_{i_j}) + \kappa \\ &\leq 2h(P_{j\text{-}1}) + \kappa' + \kappa \end{aligned}$$

where κ is another constant. From this, we get that:

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

If we now assume $h(P_{j\text{-}1}) \geq \kappa' + \kappa$ we get that

$$h(P_j) \leq \tfrac{3}{4}h(P_{j\text{-}1}),$$

meaning that the sequence of $h(P_j)$'s converges to zero, meaning that we can find an m such that $h(P_m) \leq \kappa' + \kappa$. Using (*) we now know that we can write every $P \in \Gamma$ as

$$P = 2^{\mathrm{m}}R + a_n Q_n + \ldots + a_2 Q_2 + a_1 Q_1,$$

for $a_1, \ldots, a_n$ integers and $R \in \Gamma$ such that $h(R) \leq \kappa' + \kappa$.
Therefore the set

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

generates Γ and since it is finite we are done. □

3 Concluding the Proof

First, let us restate the version of Mordell's theorem that we now can fully prove:

Theorem 3 (for curves with a rational point of order two)**.** *Let C be a non-singular cubic curve given by*

$$C : y^2 = x^3 + ax^2 + bx \quad a, b \in \mathbb{Z} \ .$$

Then the group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.

Proof. From the lemma 2.1, lemma 2.2 and lemma 3.1 from the last talk [3] (which are lemma 3.1, lemma 3.2 and lemma 3.3 in [1]) and the first part of this talk we know that we have all the requirements to apply the Descent Theorem on $C(\mathbb{Q})$. Therefore, $C(\mathbb{Q})$ is finitely generated. □

Finding the Generators

One might ask, how to go about finding these finitely many generators. The unfortunate and unsatisfactory answer is that there is no procedure that is guaranteed to work in every case. However, by using some of the methods that were used in the proof of Mordell's theorem, one can often succeed after all.

Free Rank

Since $C(\mathbb{Q})$ is a finitely generated group, we can write it as:

$$\mathbb{Z}^r \oplus \bigoplus_{i=1}^{l} \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}.$$

While we understand the torsion part pretty well (the second talk on points of finite order was in principle about that), the free part and the free rank is much harder to understand. If the rank is 0, the $C(\mathbb{Q})$ is finite. One example for this is the elliptic curve

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

where $C(\mathbb{Q})$ contains (0,0), (1,0), (-1,0), all of order 2 and O and so is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [4]. There is a conjecture that the rank can be arbitrarily large. The elliptic curve with the highest rank ever found is:

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9,$$

which has rank at least 28 [5].

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).

[2] M. Imris and N. Navea de Grahl, https://people.math.ethz.ch/ mschwagen/ellipticcurves2023/talk2pointsoffiniteorder.pdf.

[3] J. Roshardt and M. Schlatter, https://people.math.ethz.ch/ mschwagen/ellipticcurves2023/talk3heights.pdf.

[4] K. Rubin and A. Silverberg, https://www.ams.org/journals/bull/2002-39-04/S0273-0979-02-00952-7/S0273-0979-02-00952-7.pdf

[5] N. D. Elkies, *Three lectures on elliptic surfaces and curves of high rank.* Lecture notes, Oberwolfach (2007) arXiv:0709.2908

[6] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees* Proc. Camb. Philos. Soc. 21, 179–192 (1922; JFM 48.1156.03)

[7] J. W. S. Cassels, *Louis Joel Mordell, 1888-1972* Biogr. Mems Fell. R. Soc.19493-520 (1973)

[8] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions.* Proc. Camb. Philos. Soc. 19, 117–124 (1917; JFM 46.0605.01)

[9] S. Lang, *The Mordell-Weil Theorem. In: Fundamentals of Diophantine Geometry.* Springer, New York, NY. (1983) https://doi.org/10.1007/978-1-4757-1810-2_6