Mordell's Theorem

Elias Dubno and Emie Sun

November 9, 2020

1 Introduction

Throughout the first three chapters of these notes, we closely follow Silverman and Tate [2, Chapter 3.1 - 3.5].

Our goal is to prove the following theorem due to Mordell.

Theorem 1 (Mordell's Theorem)**.** *Let $C: \ y^2 = x^3 + ax^2 + bx + c$ be a non-singular cubic curve, where a, b and c are integers. Then the set of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.*

In order to prove *Mordell's Theorem*, we show that $C(\mathbb{Q})$ satisfies the conditions of the *Descent Theorem.*

Theorem 2 (Descent Theorem)**.** *Let Γ be an abelian group, and suppose that there exists a function h from Γ to the non-negative real numbers satisfying the following four conditions:*

1. *For all $M \in \mathbb{R}$, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite. ("The function h satisfies the Finiteness Property.")*
2. *For all $P_0 \in \Gamma$ there is a constant κ_0 such that for all $P \in \Gamma$, we have*
$$h(P + P_0) \leq 2h(P) + \kappa_0.$$
3. *There exists a constant κ such that for all $P \in \Gamma$, we have*
$$h(2P) \geq 4h(P) - \kappa.$$
4. *The subgroup $2\Gamma = \{P + P : P \in \Gamma\}$ has finite index in Γ.*

Then the group Γ is finitely generated.

In our case, the function h is the small height function. We know that $C(\mathbb{Q})$ is an abelian group, and we have already seen in the last talk that the first three conditions are satisfied.

It remains to show the *Descent Theorem* and to prove the fourth condition. We start with the *Descent Theorem.*

2 Proof of the Descent Theorem

Suppose we have an abelian group Γ and a function h as described above. By condition 4, there are n cosets of 2Γ in Γ for some $n \in \mathbb{N}$, and we can pick coset representatives $Q_1, \ldots, Q_n$.

Now let P be any element in Γ. Since P has to be in one of the cosets, there exists $i_1 \in \{1, \ldots, n\}$ and $P_1 \in \Gamma$ such that

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

Similarly, when starting with P_1 instead of P, we find an index $i_2 \in \{1, \ldots, n\}$ and a point $P_2 \in \Gamma$ such that

$$P_1 - Q_{i_2} = 2P_2.$$

Continuing this procedure yields a set of equations

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

where $m \in \mathbb{N}$, $Q_{i_1}, \ldots, Q_{i_m}$ are chosen from the set of coset representatives $\{Q_1, \ldots, Q_n\}$, and $P_1, \ldots, P_m$ are elements of Γ.
Note that we can rewrite the equations from above to get

$$\begin{aligned} P &= Q_{i_1} + 2P_1 \\ P &= Q_{i_1} + 2Q_{i_2} + 4P_2 \\ &\cdots \\ P &= Q_{i_1} + 2Q_{i_2} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m. \end{aligned}$$

We see that P is in the subgroup generated by the coset representatives and P_m. Now we show that by choosing m large enough, the height of the point P_m will always be less than some fixed bound $K \in \mathbb{R}$, where K does not depend on the initial starting point P. Then the set $\{Q_1, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq K\}$ is a

finite set by conditions 1 and 4 and generates Γ. It remains to find such a K.

Let us consider the sequence $P, P_1, P_2, \dots$ and let us compare the height of two successive points in this sequence. We want to show that the height significantly decreases along the sequence.
If we apply condition 2 to the point $-Q_i$ instead of P_0, we get a constant κ_i such that for all $P \in \Gamma$, we have

$$h(P - Q_i) \leq 2h(P) + \kappa_i.$$

Since there are only finitely many $Q_1, \dots, Q_n$, we can take the maximum of the numbers $\kappa_1, \dots, \kappa_n$ and call it κ'. Then for all $i \in \{1, \dots, n\}$ and for all $P \in \Gamma$, we have

$$h(P - Q_i) \leq 2h(P) + \kappa'. \tag{2.1}$$

Now let κ be the constant from condition 3. Combining condition 3 and equation (2.1) yields

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

and hence

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

It follows that whenever $h(P_{j-1}) \geq \kappa + \kappa'$, the next point P_j has strictly smaller height than its predecessor P_{j-1}, namely $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. So if we start with any point P_1 and we keep on multiplying $\frac{3}{4}$ to $h(P_1)$, we see that the sequence $\big(h(P_j)\big)_{j\in\mathbb{N}}$ would converge to 0, and hence we eventually end up with some $m \in \mathbb{N}$ such that $h(P_m) \leq \kappa + \kappa'$.

Therefore, we can write

$$\begin{aligned} P &= Q_{i_1} + 2Q_{i_2} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m \\ &= a_1 Q_1 + \cdots + a_n Q_n + 2^m P_m, \end{aligned}$$

where $a_1, \dots, a_n \in \mathbb{N}_0$ and $h(P_m) \leq \kappa + \kappa'$.

Hence the set $\{Q_1, \dots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa + \kappa'\}$, which is finite by conditions 1 and 4, generates Γ. This concludes the proof of the *Descent Theorem*.

We will now move on to prove that $\mathbb{C}(\mathbb{Q})$ satisfies condition 4 of the *Descent Theorem*.

3 Proof of Condition 4

Our goal is to show that the fourth condition in the *Descent Theorem* holds in the setting of *Mordell's Theorem*. For this, we follow the proof given in [2, Chapter 3.4 - 3.5]. closely.

Lemma 3. *Let C be a non-singular elliptic curve. Then we have*

$$(C(\mathbb{Q}) : 2C(\mathbb{Q})) < \infty.$$

Proof. Assume that our curve is in the Weierstrass form

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Z}$. We do not prove the general case. We assume that $f(x)$ has a rational point x_0. This is equivalent to $f(x)$ having an integer root because $f(x)$ is a monic polynomial with integer coefficients. It is also equivalent to $(x_0, 0)$ being a rational point of order 2. We have seen this in the talk about points of finite order. The reason for this assumption is that we do not develop the tools in algebraic number theory that we would need for the general proof.
Now we move $(x_0, 0)$ to the origin $(0, 0)$ by a linear change of coordinates. As we have seen in the talk about the Weierstrass normal form, this does not affect the group $C(\mathbb{Q})$. Hence we may assume that the elliptic curve C has the form

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

for $a, b \in \mathbb{Z}$.
Since C is non-singular, the discriminant $\mathrm{Disc}(f(x)) = b^2(a^2 - 4b)$ is nonzero. Equivalently, $b \neq 0$ and $a^2 - 4b \neq 0$.
We want to understand the multiplication by 2 map better because it obviously plays a big role in the proof of Lemma 3. We have seen in the talk on the group structure on elliptic curves that the multiplication by 2 map is

$$\begin{aligned} m : \ & C \to C \\ & P = (x, y) \mapsto 2P = (\tilde{x}, \tilde{y}) = \left(\frac{(x^2 - b)^2}{4y}, \tilde{y} \right). \end{aligned}$$

We see that the largest power of x that occurs in $\tilde{x}$ is 4, so we can call m a degree 4 map. In order to understand m, we find a decomposition of m into two degree 2 maps. Before we do that, we introduce a lemma that explains why we want to find this decomposition.

Lemma 4. *Let A, B be two abelian groups. Suppose that $\Phi : A \to B$ and $\Psi : B \to A$ are two homomorphisms such that $\Psi(\Phi(a)) = 2a$ for all $a \in A$. Moreover, suppose that $(B : \Phi(A)) < \infty$ and $(A : \Psi(B)) < \infty$. Then $(A : 2A) < \infty$.*

Proof. Let $a_1, ..., a_n$ be representatives of the cosets in $A/\Psi(B)$, i.e. for all $a \in A$ there is an unique a_i such that $a - a_i \in \Psi(B)$. Similarly, let $b_1, ..., b_m$ be representatives of the cosets in $B/\Phi(A)$. Define the set

$$S = \{a_i + \Psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}.$$

We claim that S contains a system of representatives of the cosets in $A/2A$, i.e. for all $a \in A$ there exists some $s \in S$ such that $a - s \in 2A$.
Let $a \in A$ be arbitrary. There exists some a_i such that $a - a_i \in \Psi(B)$. Equivalently, there exists some $b \in B$ such that $a - a_i = \Psi(b)$. Furthermore, there exists a b_j such that $b - b_j \in \Phi(A)$. So we can find $a' \in A$ with $b - b_j = \Phi(a')$. Thus we obtain the following equation

$$a - a_i = \Psi(b) = \Psi(\Phi(a') + b_j) = \Psi(\Phi(a')) + \Psi(b_j) = 2a' + \Psi(b_j).$$

It follows that $a = a_i + \Psi(b_j) + 2a'$. □

3.1 Definition of Ψ and Φ

In this subsection, we find the decomposition of the multiplication by 2 map m. For this, we introduce two new elliptic curves:

$$\overline{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$
$$\overline{\overline{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x,$$

where $\bar{a} = -2a,\ \bar{b} = a^2 - 4b,\ \bar{\bar{a}} = -2\bar{a} = 4a$ and $\bar{\bar{b}} = \bar{a}^2 - 4\bar{b} = 16b$. Hence $\overline{\overline{C}}$ has the form

$$\overline{\overline{C}} : y^2 = x^3 + 4ax + 16bx. \tag{3.1}$$

For simplicity, we write $\Gamma = C(\mathbb{Q})$, $\overline{\Gamma} = \overline{C}(\mathbb{Q})$, $Q = (0,0) \in \Gamma$ and $\overline{Q} = (0,0) \in \overline{\Gamma}$. We define

$$\phi : C \to \overline{C}$$
$$P = (x,y) \mapsto \begin{cases} (\frac{y^2}{x^2}, y(\frac{x^2-b}{x^2})) & \text{if } x \neq 0, \\ \mathcal{O} & \text{if } P \in \{Q, \mathcal{O}\}. \end{cases}$$

In the same way, we define $\overline{\Phi} : \overline{C} \to \overline{\overline{C}}$. To define, $\Psi : \overline{C} \to C$, we first find an isomorphism between $\overline{\overline{C}}$ and C. By (3.1), we see that the map

$$\tau : \overline{\overline{C}} \to C$$
$$P = (x,y) \mapsto \begin{cases} (\frac{1}{4}x, \frac{1}{8}y) & \text{if } P \neq \overline{\overline{\mathcal{O}}}, \\ \overline{\mathcal{O}} & \text{if } P = \overline{\overline{\mathcal{O}}}, \end{cases}$$

is an isomorphism. Hence we define $\Psi = \tau \circ \overline{\Phi}$, which is given by

$$P = (\bar{x}, \bar{y}) \mapsto \begin{cases} (\frac{1}{4}\frac{\bar{y}^2}{\bar{x}^2}, \frac{1}{8}\bar{y}(\frac{\bar{x}^2-b}{\bar{x}^2})) & \text{if } \bar{x} \neq 0, \\ \mathcal{O} & \text{if } P \in \{\overline{Q}, \overline{\mathcal{O}}\}. \end{cases}$$

Proposition 5. *The maps Φ and Ψ satisfy the following:*

1. *Φ is a homomorphism and its kernel consists of Q and $\mathcal{O}$.*
2. *$\Psi \circ \Phi = m$.*

Proof. 1. From the definition of Φ, it is clear that $\{Q, \mathcal{O}\}$ is its kernel. The proof that Φ is a homomorphism can be found in [2, Proposition 3.7].

2. Let P be a point in C. If $P = \mathcal{O}$, then it is clear that $\Psi(\Phi(\mathcal{O})) = \mathcal{O} = 2\mathcal{O}$. If $P = Q$, then $\Psi(\Phi(Q)) = \mathcal{O} = 2Q$ because Q is a point of order 2. So assume that $P = (x, y)$ with $x \neq 0$. It follows that

$$2P = 2(x, y) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3} \right).$$

Now we compute $\Psi(\Phi((x, y)))$. We know that

$$\Phi((x, y)) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2} \right),$$

so

$$\Psi(\Phi((x, y))) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4-x^4(a^2-4b))}{8y^3x^2} \right).$$

By the definition of C, P satisfies $y^4 = x^2(x^2+ax+b)^2$. It follows that

$$\Psi(\Phi((x, y))) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^2(x^2+ax+b)^2-x^4(a^2-4b))}{8y^3x^2} \right).$$

Together with

$$\begin{aligned} &x^2(x^2+ax+b)^2 - x^4(a^2-4b) \\ &= x^6 + a^2x^4 + b^2x^2 + 2ax^5 + 2bx^4 + 2abx^3 - a^2x^4 + 4bx^4 \\ &= x^6 + b^2x^2 + 2ax^5 + 2abx^3 + 6bx^4 \\ &= x^2(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2), \end{aligned}$$

it follows that $\Psi(\Phi((x, y))) = 2(x, y)$. □

Recall that our goal is to show that $(\Gamma, 2\Gamma) < \infty$. We want to show this by using Lemma 4. Hence in the setting of Lemma 4, $A = \Gamma$ and $B = \overline{\Gamma}$. We need to show that $\Phi(\Gamma) \subset \overline{\Gamma}$ and that $\Psi(\overline{\Gamma}) \subset \Gamma$. To see this, we just look at the definitions of Φ and Ψ. They obviously send rational points to rational points. Therefore, the last thing to show in order to apply Lemma 4 is that the indices $(\overline{\Gamma} : \Phi(\Gamma))$ and $(\Gamma : \Psi(\overline{\Gamma}))$ are finite. To show this, we need to first understand how the groups $\Phi(\Gamma)$ and $\Psi(\overline{\Gamma})$ look like.

Lemma 6. *The group $\Phi(\Gamma)$ is given by*

1. $\overline{\mathcal{O}} \in \Phi(\Gamma)$,
2. $\overline{Q} \in \Phi(\Gamma) \Leftrightarrow \bar{b} = a^2 - 4b$ *is a perfect square,*
3. $\overline{P} = (\bar{x}, \bar{y})$, $\bar{x} \neq 0$, *is in $\Phi(\Gamma)$ if and only if $\bar{x} = q^2$ for some $q \in \mathbb{Q}$.*

Proof. 1. The neutral element $\mathcal{O} \in \Gamma$ satisfies $\Phi(\mathcal{O}) = \overline{\mathcal{O}}$.

2. Note that $\overline{Q} \in \Phi(\Gamma)$ if and only if there exists some $P = (x, y)$ with $x \neq 0$ and $\Phi(P) + \overline{Q}$. It is clear that $\overline{Q}$ can not be the image under Φ of Q or $\mathcal{O}$. Furthermore, there exists some $P = (x, y)$ with $x \neq 0$ and $\Phi(P) + \overline{Q}$ if and only if the equation
$$0 = x^3 + ax^2 + bx$$
has a non-zero rational solution. This is equivalent to saying that $0 = x^2 + ax + b$ has a rational solution, which is true if and only if $a^2 - 4b$ is a perfect square.

3. Assume that $\overline{P} = (\bar{x}, \bar{y})$, $\bar{x} \neq 0$, is in $\Phi(\Gamma)$. Then there exists $(x, y) \in \Gamma$, $x \neq 0$, with $\Phi(x, y) = (\frac{y^2}{x^2}, ...) = (\bar{x}, \bar{y})$. Since $\frac{y^2}{x^2} = \bar{x}$, it immediately follows that $\bar{x}$ is the square of a rational number.

   Conversely, assume that $\overline{P} = (w^2, \bar{y}) \in \overline{\Gamma}$ for $w \in (\mathbb{Q}^*)^2$. Our goal is to show that $\overline{P}$ lies in the image of Φ. One can check that the point (x, y) for
$$x = \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right),\ y = xw$$
is an element in Γ and maps to $\overline{P}$ under Φ. □

By symmetry, the above Lemma also holds for $\Psi(\overline{\Gamma})$. So we know that $\Psi(\overline{\Gamma})$ consists of the points

$$\Psi(\overline{\Gamma}) = \{(x, y) \in \Gamma \mid x \text{ is a non-zero rational square}\} \cup \{\mathcal{O}\} \qquad (3.2)$$
$$[\ \cup \{Q\} \text{ if } b \text{ is a perfect square }].$$

Now that we have this explicit description of $\Psi(\overline{\Gamma})$, we can prove $(\Gamma : \Psi(\overline{\Gamma})) < \infty$. The fact that $(\overline{\Gamma} : \Phi(\Gamma)) < \infty$ then follows in exactly the same way.

For this, we define the following map:

$$\begin{aligned} \alpha : \ \Gamma &\to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ \mathcal{O} &\mapsto 1 \\ Q &\mapsto b \\ (x, y) &\mapsto x, \text{ if } x \neq 0. \end{aligned}$$

We are almost done now.

Proposition 7.

1. *The map α is a homomorphism, and its kernel is* $\ker(\alpha) = \Psi(\overline{\Gamma})$. *Therefore, α induces an injective homomorphism*

$$\Gamma/\Psi(\overline{\Gamma}) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

2. *Let $p_1, \ldots, p_t$ be the distinct prime factors of b. Then*

$$\alpha(\Gamma) \subseteq \Big\{ \pm p_1^{\epsilon_1} \ldots p_t^{\epsilon_t} : \epsilon_1, \ldots, \epsilon_t \in \{0, 1\} \Big\}.$$

3. *The index $(\Gamma : \Psi(\overline{\Gamma}))$ is at most 2^{t+1}.*

Proof.

1. From equation (3.2), it follows directly that $\ker(\alpha) = \Psi(\bar{\Gamma})$. We refer to [2, Proposition 3.8] for a detailed proof.

2. Note that $\alpha(\mathcal{O}) = 1$ as well as $\alpha(Q) = b$ are congruent to $\prod_{i=1}^{t} p_i^{\epsilon_i}$ modulo $(\mathbb{Q}^*)^2$ for some $\epsilon_i \in \{0, 1\}$.

   Let us consider a point $(x, y) \in \Gamma$ with $x \neq 0$. We already know that there exist $e, m, n \in \mathbb{Z}$ such that $(m, e) = (n, e) = 1$ and $(x, y) = (\frac{m}{e^2}, \frac{n}{e^3})$. Then the formula for our cubic curve C becomes

$$n^2 = m(m^2 + ame^2 + be^4). \tag{3.3}$$

   Note that $\alpha\big((x, y)\big) = x = \frac{m}{e^2} \equiv m \pmod{(\mathbb{Q}^*)^2}$. We can decompose m into prime factors:

$$m = p_1^{\nu_1} \ldots p_t^{\nu_t} \cdot p_{t+1}^{\nu_{t+1}} \ldots p_s^{\nu_s}, \ \nu_i \in \mathbb{N}_0.$$

   Now let $i \in \{1, \ldots, s\}$ be an index with $\nu_i > 0$. Since $p_i^{\nu_i} \mid m$, it follows by equation (3.3) that $p_i^{\nu_i} \mid n^2$.

We remark that whenever a prime p divides m, we have the following equivalence:

$$p \mid m^2 + ame^2 + be^4 \iff p \mid be^4 \overset{(m,e)=1}{\iff} p \mid b.$$

Since $p_i^{\nu_i} \mid n^2$, there are two cases:

(a) $p_i \nmid (m^2 + ame^2 + be^4) \iff p_i \nmid b$. In this case, ν_i is the highest power of p_i dividing n^2. Hence ν_i is even.

(b) $p_i \mid (m^2 + ame^2 + be^4) \iff p_i \mid b$.

In conclusion, we can write

$$m \equiv \pm \prod_{p_i \nmid b} p_i^{\nu_i} \cdot \prod_{p_i \mid b} p_i^{\nu_i} \equiv \pm p_1^{\nu_1 \pmod 2} \dots p_t^{\nu_t \pmod 2} \pmod{(\mathbb{Q}^*)^2}.$$

3. This follows directly from $\left|\left\{\pm p_1^{\epsilon_1} \dots p_t^{\epsilon_t} : \epsilon_1, \dots, \epsilon_t \in \{0,1\}\right\}\right| = 2^{t+1}$. □

In conclusion, we proved condition 4 of the *Descent Theorem* in the setting of *Mordell's Theorem*. Hence, our proof of *Mordell's Theorem* is finished.

4 Rank of Elliptic Curves

Since $C(\mathbb{Q})$ is a finitely generated abelian group, we know that

$$C(\mathbb{Q}) \cong C(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

where $C(\mathbb{Q})_{tors}$ is the finite subgroup of rational points of finite order and $r \in \mathbb{N}_0$ is some non-negative integer called the *rank* of the curve C.

The torsion part is well-understood. Using the *Nagell-Lutz Theorem*, it is relatively easy to characterize these points.

However, the rank of an elliptic curve is a rather mysterious number. There is no known algorithm guaranteed to determine the rank of a given elliptic curve. Also, it is not known which integers can be obtained as the rank of an elliptic curve, but it is a folklore conjecture that there is no maximum rank for elliptic curves. It is also widely believed that curves with large rank are very rare, and that in some asymptotic sense, the average rank of elliptic curves is $\frac{1}{2}$. In other words, it is believed that "half" of the curves have rank 0 (which is equivalent to $C(\mathbb{Q}) = C(\mathbb{Q})_{tors}$ being a finite group), "half" of the curves have rank 1, and some exceptional curves have (arbitrarily) high rank, but they do not contribute to the average because they are so rare.

The highest known rank of an elliptic curve is at least 28. This example was found by Elkies, and it is given by

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

References

[1] A. Dujella, *History of elliptic curves rank records*, `https://web.math.pmf.unizg.hr/~duje/tors/rk28.html`

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

[3] Wikipedia, *Rank of an elliptic curve*, `https://en.wikipedia.org/wiki/Rank_of_an_elliptic_curve`