THE MORDELL-WEIL THEOREM

SAMMY ROSS

1. Topic Summary

We will first introduce the claim of the Mordell-Weil theorem and explain its significance in the study of elliptic curves, before building up to the proof of the result. Our claim of the theorem will focus on the case of rational points on elliptic curves rather than $K-$rational points on algebraic varieties for simplicity; the only knowledge outside of Euler Circle that may be needed in reading the bulk of this paper is basic knowledge on projective spaces, which we refer to [4] for; however, additional knowledge is required to understand the proof of the Weak Mordell-Weil Theorem.

2. The Mordell-Weil Theorem

In class, we discussed the structure of elliptic curves through the lens of its group law. The Mordell-Weil Theorem serves as a vital foundation in the study of elliptic curves, as we understand the structure of finitely generated abelian groups very well.

Theorem 2.1 (The Mordell-Weil Theorem)**.** *The group of rational points on an elliptic curve is a finitely generated abelian group.*

In solving problems about elliptic curves, it is useful to know the properties of finitely generated-ness because it both allows us to interpret our elliptic curve group as (isomorphic to) the direct product of a finite number of cyclic groups (by the Fundamental Theorem of Finitely Generated Abelian Groups).

To prove the Mordell-Weil Theorem traditionally, we first prove the "Weak Mordell-Weil Theorem" stating that the quotient group of an elliptic curve with a multiple of said curve is finite. Next, we define a condition for an abelian group G to be finitely generated (given G/mG is finite) through the usage of height functions. We finally construct a height function on our elliptic curve, which implies the Mordell-Weil Theorem.

3. The Weak Mordell-Weil Theorem

We will provide the groundworks to understand the intuitive behind the Weak Mordell-Weil theorem, but refer to [1] or [3] for a complete proof.

Theorem 3.1 (The Weak Mordell-Weil Theorem)**.** *For any $m > 2$, the quotient group $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite.*

Date: December 11, 2023.

Note if we assume the Mordell-Weil Theorem is true, the weak theorem follows directly from observing the generators of the elliptic curve; if there are n generators of E, there are at most m^n points in E/mE, which is why the "weak" labelling is appropriate.

The proof of this theorem requires significant machinery outside of what we covered in class, so our sketch will emphasize the ideas implemented in its proof while handwaving through its more technical parts, though advanced knowledge (Galois cohomology) is still required to understand the outline of our proof. We refer to [2] for curious readers in learning more background on the proof, but for those less patient it may be worth moving directly to the next section of our proof. Here, we will let K be an arbitary number field instead of focusing solely on $\mathbb{Q}$.

We cite the following theorem from Kummer Theory without proof from [2]:

Theorem 3.2. $\mathrm{Hom}_c(G_K, \mu_n) = K^*/(K^*)^n$, *where K is a number field, $G_K = \mathrm{Gal}(\overline{K}/K)$, μ_n is the group of the nth roots of unity in K, and K^* is the dual of K (as $\mathbb{Q}$ vector spaces). See (1) pg 1 of [2]*

This is implemented in the proof of the Weak Mordell-Weil Theorem as a part of a long exact sequence used to obtain the exact sequence presented later in this paper.

Now, we define Selmer and Tate-Shafarevich Groups, which define an exact sequence later on that is used to prove our theorem.

Definition 3.3 (Selmer Group)**.** The Selmer Group, denoted $S^{(n)}(E/K)$ is defined by $S^{(n)}(E/K) = \ker(\mathrm{Hom}(G_K, E\,[n]) \to \prod_u \mathrm{Hom}(G_{K_u}, E)$

Definition 3.4 (Tate-Shafarevich Group)**.** The Tate-Shafarevich Group, denoted $III(E/K)$ is defined by $III(E/K) = \ker(\mathrm{Hom}(G_K, E) \to \prod_u \mathrm{Hom}(G_{K_u}, E)$

Note that intuitively, if $E\,[n] \subseteq E\,[K]$, that the Selmer Group embeds into the Tate-Shafarevich Group; the significance of these groups are solely in forming an exact sequence.

In fact, proving the Selmer Group is finite is an important step in proving the Weak Mordell-Weil Theorem, implementing the result from Kummer Theory by interpreting elements of $\mathrm{Hom}(G_K, E\,[n])$ as elements of $K^*/(K^*)^n$, allowing us to translate the problem into one solvable using the tools of class field theory, which we cannot come close to covering in this paper. We further refer to [2] for a more in depth explanation of this result.

The reason proving the Selmer Group is finite is important because we have the following exact sequence of cohomology, again cited without proof from [2]:

$$0 \to E(K) \to nE(K) \to S^{(n)}(E/K) \to III(E/K)\,[n] \to 0$$

This implies $E(K)/nE(K)$ embeds into the finite Selmer group and is thus finite as well; however this relies on the elements of $E\,[n]$ being in K for our sequence to be well-defined. To remedy this, we can find a finite Galois extension L of K such that $E\,[m] \subseteq E(L)$, implying $E(L)/mE(L)$ is finite. Fortunately, the finiteness of $E(K)/mE(K)$ follows from $E(L)/mE(L)$ being finite (Lemma 3.3, [1]), which finishes the proof.

4. Descent Argument

Finally, we will move to the main emphasis of the paper: proving the Mordell-Weil theorem using the weak Mordell-Weil Theorem through a descent argument. We start by defining a height function and proving that any abelian group A with corresponding finite quotient group A/mA and height function h, can be generated by finitely many elements by tracking h. Thus, it is sufficient to prove that there exists a height function that is well defined on elliptic curves over the rationals, which we do to finish our proof.

For fun, we first introduce the following problem with proof, which can be solved by using an elementary descent argument; the proof of the Descent Theorem (Thrm 4.2) is very similar conceptually, albeit more technical.

Example (IMO 1988 Problem 6). For positive integers a and b such that $ab+1|a^2+b^2$, show that $\frac{a^2+b^2}{ab+1}$ is a perfect square

To prove this problem, we set $\frac{a^2+b^2}{ab+1} = k$ for fixed constant k and note that $a^2+b^2-abk-k = 0$. Assume for the sake of contradiction that $a+b$ is minimal and $a \geq b$. This is a quadratic in a with solutions $a = \frac{bk\pm\sqrt{b^2k^2+4k-4b^2}}{2}$; when $a > b$, a is equal to the larger of these solutions, which is an integer, however, $\frac{{a_1}^2+b^2}{a_1b+1} = k$ as well, where a_1 is the lesser solution. As $a_1+b < a+b$, we have a contradiction if a_1 is also positive. Thus, $a_1 = 0$ (as if it was negative, $\frac{{a_1}^2+b^2}{a_1b+1}$ would be either negative or undefined), so $\frac{{a_1}^2+b^2}{a_1b+1} = b^2$ is a perfect square.

We now introduce the definition of a height function taken from [1]:

Definition 4.1 (Height Function (Yu)). Let A be an abelian group. A height function is a map $h : A \to \mathbb{R}$ satisfying the following three properties:

(1) For each $Q \in A$, there is a constant $C_1(A,Q)$ depending on A and Q, such that $h(P+Q) \leq 2h(P) + C_1$ for any $P \in A$.

(2) There is an integer $m \geq 2$ and a constant $C_2(A)$ only depending on A, such that $h(mP) \geq m^2h(P) - C_2$

(3) For every constant C_3, the set $\{P \in A : h(P) \leq C_3\}$ is finite (this implies h is non-negative except at finitely many points).

Although the conditions for a height function may seem relatively arbitrary, they are chosen to be general to allow us to construct one on elliptic curves (and general algebraic varieties), yet precise enough to allow for the following Descent Theorem to hold, allowing us to construct (finitely many) generators for our abelian group.

Theorem 4.2 (Descent Theorem (Yu)). *If A is an abelian group such that A/kA is a finite group for some positive integer k, if there exists height function $h : A \to \mathbb{R}$ (such that $m = k$ in the second condition of a height function), then A is finitely generated.*

Proof. Let $A/mA = \{a_1, a_2, \cdots a_r\}$, and let $P_0 \in A$. For $1 \leq k \leq n$, let $P_k = mP_{k+1} + a_{i_k}$.

Then, note that $h(P_j) \leq 1/m^2(C_2 + h(mP_j)) = 1/m^2(C_2 + h(P_{j-1} - a_{i_j}))$ by property 2 of a height function, $1/m^2(C_2 + h(P_{j-1} - a_{i_j})) \leq 1/m^2(C_1 + C_2 + 2h(P_{j-1}) \leq h(P_{j-1})/2 + C$ by property 1 of a height function and using the fact $m \geq 2$ (where C is a constant depending on A and the elements of A/mA). Now, note that P_0 can be represented as the linear combination of P_n and elements of A/mA. For significantly large n, note $\frac{1}{2^n}h(P_0) < 1$, which implies $h(P_n) \leq 1+2C$, as otherwise we could reverse our descent (assuming $h(P_n) > 1+2C$) to find the contradiction that $h(P_0) > 1$. As C is a constant, by property 3 of a height function we can note there exists only finitely many potential P_n; thus as we can express any point P_0 as a linear combination of the finitely many elements of A/mA and finitely many options for P_n, A must be finitely generated. ■

Intuitively, this theorem allows us to construct generators of an abelian group G with finite G/mG given the existence of the aforementioned height function.

Example. Let G be the group $\mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}$. We know that G is finitely generated of course as it is the direct product of finitely many finitely generated groups, but assuming we do not, we can define the function $h(x, y, z) = x^2 + y^2$, where $(x, y, z) \in \mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}$. It is straightforward to then verify that h satisfies the requirements of a height function (say with $m = 2$), and thus as $(\mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}/2\mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ is finite, $\mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}$ is finitely generated.

Using the Descent Theorem and Weak Mordell-Weil theorem, it is sufficient to construct a height function on $E(\mathbb{Q})$. We first define the height and logarithmic height (of a function) on $\mathbb{Q}$, then move to showing the logarithmic height satisfies the requirements of a height function.

Definition 4.3 (Rational Height)**.** Let $x = [x_0 : x_1 \cdots : x_n] \in \mathbb{P}^n(\mathbb{Q})$, where each $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \cdots, x_n) = 1$. The height of x, $H(x) = \max_{0 \leq i \leq n} |x_i|$.

We now define h_f, which we will show is a height function on $E(\mathbb{Q})$:

Definition 4.4 (Logarithmic Height)**.** For some non-constant function $f : E \to \mathbb{P}$, let $h_f(P) = \log(H(f(P)))$. In this paper, we assume $f((x_1, y_1)) = x'$ for $(x_1, y_1) \in E(\mathbb{Q})$, and $x' = [a : b]$, where $a/b = x$, where a and b are relatively prime integers, and b is positive.

The following results can be generalized for any h_f, but for proving the Mordell-Weil theorem we only need to know the result when $f(P)$ yields the x-coordinate of $P \in E(\mathbb{Q})$. Note that the way we have defined x', $H(x') \geq 1$ so h_f must be non-negative.

We take without proof the following theorem, which can be found as Theorem 6.2 of Chapter 8 of [3] (taken from [1]).

Theorem 4.5 (Descent Lemma)**.** *For all $P, Q \in E(\mathrm{Q})$, $h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$, where the constant only depends on elliptic curve E and f.*

This theorem allows us to interpret the properties of h_f through a functional equation that has nice properties that are similar (though not necessarily the same) as a linear function.

We finally move on to proving h_f satisfies the conditions of a height function:

Corollary 4.6. *h_f satisfies the first and second conditions of a height function*

Proof. For the first condition, note that $h_f(P+Q) \leq 2h_f(P)+2h_f(Q)+O(1) = 2h_f(P)+C_1$ directly from the Descent Lemma, and that h_f is always non-negative.

For the second condition, we set $m = 2$ and note that by setting $P = Q$ in the descent lemma that $h_f(2P) = 4h_f(P) + O(1) = 4h_f(P) + C_2 \rightarrow h_f(2P) \geq 4h_f(P) + C_2$ which is sufficient. ■

Theorem 4.7 (Condition 3). *For any constant C, the set $P \in \mathbb{P}(\mathbb{Q}) : H(P) \leq C$ contains finitely many points*

Proof. Assume without loss of generality C is a positive integer. Note that for $x \in \mathbb{P}(\mathbb{Q})$ with normalized coordinates $[x_0 : x_1]$, that $H(x) = \max\{|x_0|, |x_1|\}$. When $H(x) \leq C$, we must have $|x_0| \leq C$ and $|x_1| \leq C$. As x_0 and x_1 must be integers, there are at most $2C+1$ possible values of x_0 and x_1, and thus at most $(2C+1)^2$ possible $x = [x_0 : x_1]$ when normalized, which is finite. ■

h_f satisfies the conditions of a height function (with $m = 2$) on $E(\mathbb{Q})$, thus, as $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, $E(\mathbb{Q})$ is finitely generated, proving the Mordell-Weil Theorem.

Remark 4.8. Although here we only proved the Mordell-Weil Theorem over elliptic curves and $\mathbb{Q}$, the descent argument works perfectly fine over general number fields and algebraic varieties, albeit with a couple more steps, which we again refer to [1] for.

5. Sources Implemented

[1] Yu, Huishi. A Proof of the Mordell-Weil Theorem. 21 Aug. 2021, `https://math.uchicago.edu/~may/REU2021/REUPapers/Yu,Huishi.pdf`

[2] Ji, Caleb. The Mordell-Weil Theorem. `https://math.columbia.edu/~calebji/mordell-weil.pdf`

[3] Silverman, Joseph H. The Arithmetic of Elliptic Curves. Springer, 2009

[4] Weisstein, Eric W. "Projective Space." From MathWorld–A Wolfram Web Resource. `https://mathworld.wolfram.com/ProjectiveSpace.html`

Email address: `srossthemathdragon@gmail.com`