The Mordell-Weil Theorem

1 Elliptic Curves

We begin with the definition of elliptic curves.

Definition 1.1. *An elliptic curve E over a field K, denoted by E/K is a plane curve defined by an equation $y^2 = x^3 + ax + b$ for $a, b \in K$ where the discriminant $\Delta = (4a^3 + 27b^2) \neq 0$.*

It is natural to be curious about the set $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b,\ a, b \in K,\ \Delta \neq 0\} \cup \{\infty\}$. Here, ∞ denotes the point at infinity which we naively interpret this point to lie in every line $x = c$ for all $c \in K$ with y-coordinate ∞.

In fact, $E(K)$ inherits an abelian group structure. For $P, Q \in E(K)$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and ∞. Then L' intersects E at R, ∞, and a third point which is defined as $P + Q$. Since this binary operation is obviously symmetric, it is reasonable to use the additive notation. ∞ becomes the identity and $-P$ is defined by the point obtained by reflecting P across the x-axis. Besides associative law, other group laws can be easily verified. Moreover, one can verify associative law case by case, or more elegantly, using Riemann-Roch theorem [2, III.2.2].

The group $E(K)$ is called the *Mordell-Weil group* of E/K. So naturally, our concern is to compute the Mordell-Weil group. Although an elliptic curve can be defined over an arbitrary number field K, we mostly focus on the case $K = \mathbb{Q}$.

2 The Mordell-Weil Theorem

Theorem 2.1. *(Mordell-Weil) For a number field K, the abelian group $E(K)$ is finitely generated.*

We prove it for the case $K = \mathbb{Q}$. The proof of the Mordell-Weil theorem consists of two parts: the first part is to prove the weak Mordell-Weil theorem and the second part is to prove the decent theorem to complete the proof.

Theorem 2.2. *(Weak Mordell-Weil) For a number field K, an elliptic curve E/K, and any integer $m \geq 2$, $E(K)/mE(K)$ is a finite group.*

Note that the weak Mordell-Weil theorem is not enough to prove the Mordell-Weil theorem. For example, for every positive integer m, $\mathbb{R}/m\mathbb{R} = 0$ is finite yet $\mathbb{R}$ is not a finitely genereted abelian group. The problem occurs since there are large number of elements divisible by m so that we obtain a finite group even after we mod out those elements. To resolve this problem, we consider a particular situation that we can give a restriction to the number of elements using so called 'height'. To be specific, we introduce the decent theorem which is worthwhile to prove.

Theorem 2.3. *(Decent Theorem) Let A be an abelian group. Suppose that there exists a (height) function*

$$h : A \to \mathbb{R}$$

with the following properties:
(a) Let $P_0 \in A$. There is a constant C_1, depending on A and P_0, such that

$$h(P + P_0) \leq 2h(P) + C_1 \textit{ for all } P \in A$$

(b) There are an integer $m \geq 2$ and a constant C_2, depending on A, such that

$$h(mP) \geq m^2 h(P) - C_2 \textit{ for all } P \in A$$

(c) For every constant C_3, the set

$$\{P \in A : h(P) \leq C_3\}$$

is finite.
Suppose further that for the integer m in (b), the quotient group A/mA is finite. Then A is finitely generated.

Proof. Let Q_i, $1 \leq i \leq r$ be representatives of cosets in A/mA. Note that for each $P \in A$, there exists $P' \in A$ and Q_i such that $P = mP' + Q_i$. Let $P \in A$ be given. Define P_i inductively as follows.

$$\begin{aligned} P =& mP_1 + Q_{i_1} \\ P_1 =& mP_2 + Q_{i_2} \\ &\vdots \\ P_{n-1} =& mP_n + Q_{i_n} \end{aligned}$$

Let C_1' be a maximal constant among the constants from (a) for all Q_i's. By (a) and (b), we have

$$h(P_j) \leq \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2)$$

Using this inequality repeatedly, we get

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2) \\ &< \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \text{ since } m \geq 2 \end{aligned}$$

Therefore, for sufficiently large n, we have

$$h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2)$$

Moreover, since P is a linear combination of P_n and Q_i's, it follows that A is generated by

$$\{Q_i : i = 1, \cdots, r\} \cup \{Q : h(Q) \leq 1 + \frac{1}{2}(C_1' + C_2)\}$$

which is finite by (c). □

Combining the weak Mordell-Weil theorem and the decent theorem, one can see that it is enough to find an integer $m \geq 2$ and a height function on a Mordell-Weil group to prove the Mordell-Weil theorem. Although the Mordell-Weil theorem is true for an arbitrary number field, first consider the case $K = \mathbb{Q}$. Now we define a height function on the Mordell-Weil group as follows.

Definition 2.4. *The (logarithmic) height on $E(\mathbb{Q})$ is the function $h_x : E(\mathbb{Q}) \to \mathbb{R}$ defined by*

$$h_x(P) = \begin{cases} logH(x(P)) & P \neq \infty \\ 0 & P = \infty \end{cases}$$

where $x(P)$ is the x-coordinate of P and $H(t) = max(|p|, |q|),\ t = p/q \in \mathbb{Q}$ is a fraction in lowest term. H(t) is called the height of t. Note that h_x is positive.

So the proof of the Mordell-Weil theorem is completed by verifying that the logarithmic height function on $E(\mathbb{Q})$ satisfies assumptions of the decent theorem. The integer in (b) will be $m = 2$. First, (c) can be easily verified since given constant C, there are at most $(2C+1)^2$ possible $x \in \mathbb{Q}$ satisfying $H(x) < C$ and given x, there are at most two values of y such that $(x, y) \in E(\mathbb{Q})$. Proofs of (a) and (b) can be developed not that hard if one can note that $(x, y) \in E(\mathbb{Q})$ has a reduced form $(a/c^2, b/c^3)$. Proofs can be found in [2, VIII.4.1]. Lastly, finiteness of the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is guaranteed by the weak Mordell-Weil theorem. One can define a height function on an elliptic curve over an arbitrary number field to use the decent theorem similarly. So the Mordell-Weil theorem is proved.

3 Remarks

From the Mordell-Weil theorem, we can compute the Mordell-Weil group if we compute finitely many generators for it. Recall the proof of the decent theorem. First, we need to find out the representatives $\{Q_i\}$ of cosets in $E(K)/mE(K)$ and calculate constants C_1 for each Q_i. Furthermore, we must be able to calculate constants C_2 and C_3. In fact, given generators for $E(K)/mE(K)$, a finite amount of computation yields generators for $E(K)$ since it is able to compute those constants effectively. We will see these relations later concerning the proof of the weak Mordell-Weil theorem which is based on the Kummer paring. After all, so the problem of computing the Mordell-Weil group reduces to the problem of computing the weak Mordell-Weil group $E(K)/mE(K)$. Unfortunately, there is no currently known algorithm to compute generators. However, we build several methods to approach this problem, for example, the Selmer group and the Shafarevich-Tate group.

References

[1] Rajan, C. S.,*Weak Mordell-Weil theorem. In: Bhandari A.K., Nagaraj D.S., Ramakrishnan B., Venkataramana T.N. (eds) Elliptic Curves, Modular Forms and Cryptography.* Hindustan Book Agency, Gurgaon, 2003

[2] Silverman, J. H., *The Arithmetic of Elliptic Curves.* 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009

[3] Silverman, J. H., Tate, J. T., *Rational Points on Elliptic Curves.* 2nd ed., Undergraduate Texts in Mathematics, Springer International Publishing, 2015