A Height Function on $E(\mathbb{Q})$

Myeong Jae Jeon

Abstract

The Mordell-Weil theorem says that an abelian group $E(K)$ is finitely generated for any number field K . The proof of Mordell-Weil theorem consists of two parts. The first one is showing the existence of the height function on an elliptic curve satisfying certain properties, and the second one is the proof of the weak Mordell-Weil theorem. Combining these two results, the descent theorem tells us immediately that $E(K)$ is finitely generated. We will prove the Mordell-Weil theorem for elliptic curves over the rational field. In this article, we prove the first part of the proof: the existence of the height function on $E(\mathbb{Q})$ satisfying the desired properties.

1 Existence of a certain height function on $E(\mathbb{Q})$

Our goal in this article is to define a height function on $E(\mathbb{Q})$ satisfying certain properties. To specify these properties, recall the descent theorem as follows.

Theorem 1.1 (Descent Theorem)**.** *Let A be an abelian group. Suppose that there exists a (height) function*

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

with the following properties:
(a) For every constant C_1, the set

$$\{P \in A : h(P) \leq C_1\}$$

is finite.
(b) Let $P_0 \in A$. There is a constant C_2, depending on A and P_0, such that

$$h(P + P_0) \leq 2h(P) + C_2 \text{ for all } P \in A$$

(c) There are an integer $m \geq 2$ and a constant C_3, depending on A, such that

$$h(mP) \geq m^2 h(P) - C_3 \text{ for all } P \in A$$

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

In our cases, the abelian group A in the theorem is $E(\mathbb{Q})$, so we will find a height function on $E(\mathbb{Q})$ satisfying conditions (a)-(c), in particular with $m = 2$. Then the weak Mordell-Weil theorem says that the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite and hence $E(\mathbb{Q})$ is finitely generated. We define a height function h on $E(\mathbb{Q})$ as follows and prove it is a desired height function. Here, our elliptic curve is defined by the equation $y^2 = x^3 + Ax + B$. Proofs are in increasing order of difficulty.

Definition 1.2. *The (logarithmic) height on $E(\mathbb{Q})$ is the function $h : E(\mathbb{Q}) \to \mathbb{R}$ defined by*

$$h(P) = \begin{cases} \log H(x(P)) & P \neq \infty \\ 0 & P = \infty \end{cases}$$

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 is non-negative since $x(P) \geq 1$ for all P.

Proof. (a) Given constant C, there are at most $(2C + 1)^2$ possible $x \in \mathbb{Q}$ satisfying $H(x) < C$ and given such x, there are at most two values of y such that $(x, y) \in E(\mathbb{Q})$. Hence the set given in (a) is finite.

(b) Fix $P_0 = (x_0, y_0)$ and let $P = (x, y)$ be given. We may assume $C_2 > \max\{h(P_0), h(2P_0)\}$ which guarantees that (a) is true for $P_0 = \infty$ or $P \in \{P_0, -P_0, \infty\}$. In other cases, after elementary calculation and comparing divisors of numeraters and denominators of coordinates, we can write

$$P_0 = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right), \quad P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$$

with reduced forms. On the other hand, using group laws in $E(\mathbb{Q})$, we can write

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0$$

Using the Weierstrass equation $y^2 = x^3 + Ax + b$ and coordinates, we can show that

$$\begin{aligned} x(P + P_0) &= \frac{(xx_0 + A)(x + x_0) + 2B - yy_0}{(x - x_0)^2} \\ &= \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2} \end{aligned}$$

Note that cancellation between numerator and denominator can only decrease the height, so we have an estimation

$$H(x(P + P_0)) \leq C_2' \max\{|a|^2, |d|^4, |bd|\}$$

where C_2' only depends on A, B, a_0, b_0, d_0. Note that $H(x(P)) = \max\{|a|, |d|^2\}$, so we are done unless $|bd|$ becomes the maximum on the right hand side. Meanwhile, using the fact that P is a point on the given elliptic curve, we obtain

$$b^2 = a^3 + Aad^4 + Bd^6$$

so that

$$|b| \leq C_2'' \max\{|a|^{3/2}, |d|^3\}$$

where C_2'' only depends on A, B. Consequently, combining with the previous result, we can conclude that

$$H(x(P+P_0)) \leq C_2''' \max\{|a|^2, |d|^4\} = C_2''' H(x(P))^2$$

where C_2''' only depends on $E(\mathbb{Q})$ and P_0. Taking logarithm on the both hand sides gives (b).

(c) Our method would be quite an ad hoc way for this proof. Recall that we are proving this theorem for $m = 2$. That is, we find a constant C_3 which depends on the given elliptic curve, such that

$$h(2P) \geq 4h(P) - C_3 \text{ for all } P \in E(\mathbb{Q})$$

First, choosing C_3 to satisfy

$$C_3 \geq 4 \max\{h(T) : T \in E(\mathbb{Q}), 2T = \infty\}$$

we may assume that $2P \neq \infty$. Note that the set in the right hand side is finite since $2T = \infty$ if and only if the tangent line of $E(\mathbb{Q})$ at T is parallel to the y-axis which can occur only at finitely many points. Then writing $P = (x, y)$, we can compute the coordinates of $2P$ using the group law, so we obtain

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}$$

Now we introduce an additional variable to change the polynomials in the numerator and the denominator of the above formula into homogeneous polynomials. Consider

$$F(X, Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4$$
$$G(X, Z) = 4X^3Z + 4AXZ^3 + 4BZ^4$$

Luckily, letting $x = a/b$ in a lowest forms, we have

$$x(2P) = \frac{F(a, b)}{G(a, b)}$$

The key of our proof is that $F(X, 1)$ and $G(X, 1)$ are relatively prime polynomials in $\mathbb{Q}[X]$. Indeed, we see that

$$x(2P) = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)}$$

where $f(x) = x^3 + Ax + B$ and since elliptic curves are defined to be non-singular, f and f' have no common complex roots. So, $F(X, Z)$ and $G(X, Z)$ are relatively prime homogeneous polynomials

in $\mathbb{Z}[X, Z]$. Then, since the discriminant of the elliptic curve $\Delta = 4A^3 + 27B^2 \neq 0$, we can find homogeneous polynomials f_1, f_2, g_1, g_2, satisfying

$$f_1(X, Z)F(X, Z) - g_1(X, Z)G(X, Z) = 4\Delta Z^7$$
$$f_2(X, Z)F(X, Z) - g_2(X, Z)G(X, Z) = 4\Delta X^7$$

Now, plug in $(X, Z) = (a, b)$ and let $\delta = \gcd(F(a, b), G(a, b))$, then we see that δ divides 4Δ. Hence,

$$H(x(2P)) \geq \frac{\max\{|F(a, b)|, |G(a, b)|\}}{|4\Delta|}$$

We also have the following estimates from the above identities.

$$|4\Delta b^7| \leq 2\max\{|f_1(a, b)|, |g_1(a, b)|\}\max\{|F(a, b)|, |G(a, b)|\}$$
$$|4\Delta a^7| \leq 2\max\{|f_2(a, b)|, |g_2(a, b)|\}\max\{|F(a, b)|, |G(a, b)|\}$$

On the other hand, using the Euclidean algorithm, one can find f_1, f_2, g_1, g_2 explicitly as follows

$$f_1(X, Z) = 12X^2Z + 16AZ^3$$
$$g_1(X, Z) = 3X^3 - 5AXZ^2 - 27BZ^3$$
$$f_2(X, Z) = 4(4A^3 + 27B^2)X^3 - 4A^2BX^2Z + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3$$
$$g_2(X, Z) = A^2BX^2 + A(5A^3 + 32B^2)X^2Z + 2B(13A^63 + 96B^2)XZ^2 - 3A^2(A^3 + 8B^2)Z^3$$

From this, we have estimations

$$\max\{|f_1(a, b)|, |g_1(a, b)|, |f_2(a, b)|, |g_2(a, b)|\} \leq C\max\{|a|^3, |b|^3\}$$

where C depends on A and B. So, combining above results yields

$$\max\{|4\Delta a^7|, |4\Delta b^7|\} \leq 2C\max\{|a|^3, |b|^3\}\max\{|F(a, b)|, |G(a, b)|\}$$

After cancellation,

$$H(x(2P)) \geq \frac{\max\{|F(a, b)|, |G(a, b)|\}}{|4\Delta|} \geq (2C)^{-1}\max\{|a|^4, |b|^4\} = (2C)^{-1}H(x(P))^4$$

Taking logarithms on both hand sides, we obtain the desired result. □

So our next step will be the proof of the weak Mordell-Weil theorem for $m = 2$: $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, which completes the proof of the Mordell-Weil theorem.

References

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

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