

The canonical height on an elliptic curve

Myeong Jae Jeon

Abstract

In the proof of the Mordell-Weil Theorem, we defined the height function h on elliptic curves. Motivated by quasi-quadratic nature of the height function, André Néron and John Tate constructed a quadratic form whose difference with h_f is bounded. In this article, we briefly review the construction of this quadratic form which is called the canonical height.

1 Motivation

In this section, we state a relationship between height functions and the addition law on an elliptic curve. First, we introduce "big- O " notation.

Notation 1.1. *For real-valued functions f and g on a set S , we write*

$$f = g + O(1)$$

if there exist constants C_1 and C_2 such that

$$C_1 \leq f(P) - g(P) \leq C_2 \text{ for all } P \in S$$

We write $f \geq g + O(1)$ or $f \leq g + O(1)$ if only the lower inequality or the upper inequality is true.

Theorem 1.2. *Let E/K be an elliptic curve, an f be an even function on E . Define h_f by*

$$h_f(P) = h(f(P))$$

Then for all P, Q on E and $m \in \mathbb{Z}$ the followings are true.

(a)

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + O(1)$$

where the $O(1)$ depends on E, f .

(b)

$$h_f(P + Q) \leq 2h_f(P) + O(1)$$

where the $O(1)$ depends on E, f, Q .

(c)

$$h_f(mP) = m^2 h_f(P) + O(1)$$

where the $O(1)$ depends on E, f , and m .

Theorem 1.2 shows that h_f behaves like a quadratic form up to some bounded set depending on E and f . Natural question followed by this interpretation is whether one could find an actual quadratic form that differs from h_f by a bounded amount. Indeed, Néron and Tate constructed a quadratic form whose difference with h_f is $O(1)$.

2 The Canonical Height

On their constructions on the desired quadratic form, Néron constructed it as a sum of "quasi-quadratic" local functions while Tate defined it as a simpler global form. We introduce two equivalent definitions of the canonical height.

Definition 2.1 (Néron). *Let E/K be an elliptic curve. The canonical (or Néron-Tate) height \hat{h} on E is defined by*

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P)$$

where M_K is the set of all absolute values on a number field K and λ_v is the local height function for E at v .

Definition 2.2 (Tate). *Let E/K be an elliptic curve and f be any non-constant even function. The canonical (or Néron-Tate) height \hat{h} on E/K is defined by*

$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{N \rightarrow \infty} 4^{-N} h_f(2^N P)$$

Remarkable fact is that the limit above exists and is independent of the choice of f . The following theorem shows that \hat{h} is the desired quadratic form on $E(K)$.

Theorem 2.3 (Néron, Tate). *The canonical height \hat{h} satisfies the followings.*

(a) (Parallelogram Law) *For all P, Q on E , we have*

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

(b) *For all P on E and all $m \in \mathbb{Z}$,*

$$\hat{h}(mP) = m^2 \hat{h}(P)$$

(c) *The pairing*

$$\begin{aligned} \langle \cdot, \cdot \rangle : E(\overline{K})E(\overline{K}) &\rightarrow \mathbb{R}, \\ \langle P, Q \rangle &= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \end{aligned}$$

is bilinear. The pairing is called the canonical height (or Néron-Tate) pairing on E/K

(d) The canonical height is a nonnegative function and

$$\hat{h}(P) = 0 \quad \text{if and only if} \quad P \text{ is a torsion point.}$$

(e) For an even function f on E ,

$$(\deg f)\hat{h} = h_f + O(1)$$

where the $O(1)$ depends on E and f

Theorem 2.3. (b),(c),(e) shows that the canonical height is the desired quadratic form: a quadratic form that differs from h_f by a bounded amount. On the other hand, theorem 2.3. (c),(d) shows that \hat{h} defines a positive definite quadratic form on $E(K)/E_{\text{tor}}(K)$. Note that $E(K)/E_{\text{tor}}(K)$ can be embedded into $E(K) \otimes \mathbb{R}$ as a lattice. Thanks to the Mordell-Weil theorem, $E(K) \otimes \mathbb{R}$ becomes a finite dimensional real vector space. Then the following lemma guarantees that the canonical height extends to a positive definite quadratic form on $E(K) \otimes \mathbb{R}$

Lemma 2.4. *For a finite dimensional real vector space V and its lattice L , suppose a quadratic form q on V satisfies the followings.*

(a) *For $P \in L$, we have $q(P) = 0$ if and only if $P = 0$*

(b) *For every constant C , the set*

$$\{P \in L : q(P) \leq C\}$$

is finite.

Then q is positive definite on V

By theorem 1.2., together with theorem 2.3.(c)-(e), the canonical height and the lattice $E(K)/E_{\text{tor}}(K)$ satisfy conditions of lemma 2.4. It follows that the \hat{h} extends to a positive definite quadratic form on a finite dimensional real vector space $E(K) \otimes \mathbb{R}$. Moreover, the canonical height pairing extends to a positive definite hermitian form on $E(K) \otimes \mathbb{C}$ in certain situations [1].

Meanwhile, since the canonical height is non-negative for nontorsion points, it is natural to ask the lower bound of positive canonical height. There are two fundamental conjectures about lower bounds of the canonical height given by Lang and Lehmer and it is known that the abc conjecture implies Lang's conjecture.

References

- [1] Siksek, S *The height pairing on an elliptic curve with complex multiplication.* Arab Journal of Mathematical Sciences 5 (1999), 43-48.
- [2] Silverman, J. H., *The Arithmetic of Elliptic Curves.* 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009