THE HEIGHT PAIRING ON ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

S. SIKSEK

Abstract. In this paper we show how to use the canonical height on elliptic curves with complex multiplication to construct a complex inner product on the curve. This can be used to check for the dependence of points on the curve over the order of complex multiplication.

The canonical height is an extremely powerful and versatile tool for the study of elliptic curves. The usefulness of the canonical height rests on two of its properties:

(1) That its difference from the logarithmic height is bounded. The logarithmic height is a function with measures the 'size' of the points on the curve (see [5], [6]).
(2) That the canonical height can be used to define a quadratic form which, roughly speaking, turns the elliptic curve in to a real inner product space.

We can make the second property above precise as follows: suppose that L is a number field and E is an elliptic curve defined over L. Consider the real vector space $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$; it is well known that $E(L)/E_{\text{tors}}(L)$ embeds injectively into $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$ and that the canonical height $\hat{h} : E(L) \to \mathbb{R}$ can be extended uniquely to a positive definite quadratic form on $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$, which we lazily denote by $\hat{h}$ again (see [3, page 232]). Thus $\hat{h}$ satisfies the following three properties:

(1) $\hat{h}(Q) \geq 0$ for all $Q \in \mathbb{R} \otimes_{\mathbb{Z}} E(L)$; moreover $\hat{h}(Q) = 0$ if and only if $Q = 0$.
(2) $\hat{h}(\alpha Q) = \alpha^2 \hat{h}(Q)$ for all $Q \in \mathbb{R} \otimes_{\mathbb{Z}} E(L)$ and all real α.
(3) $\hat{h}$ satisfies the parallelogram law which states that for all $Q_1,\ Q_2$ in $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$ then

$$\hat{h}(Q_1 + Q_2) + \hat{h}(Q_1 - Q_2) = 2\hat{h}(Q_1) + 2\hat{h}(Q_2)$$

One can now define a real inner product on $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$ as follows:

$$\langle Q_1, Q_2 \rangle = \frac{1}{2}(\hat{h}(Q_1 + Q_2) - \hat{h}(Q_1) - \hat{h}(Q_2))$$

.

Suppose now that E is an elliptic curve defined over a number field L, E having multiplication by $\mathcal{O}$, an order in a complex quadratic field K. Further, suppose that $E(L)$ is closed under the action of $\mathcal{O}$, thus $\alpha P \in E(L)$ for all $\alpha \in \mathcal{O}$ and $P \in E(L)$. It follows that $E(L)$ is an $\mathcal{O}$-module and it is natural to consider the complex vector space $\mathbb{C} \otimes_{\mathcal{O}} E(L)$ which we denote by $\mathcal{E}(L)$.

1991 *Mathematics Subject Classification.* 11G05; Secondary 11G15.
Key words and phrases. Canonical Height, Elliptic Curves, Complex Multiplication.
This research was conducted while the author was a research assistant at the University of Kent, and funded by a grant from the EPSRC (UK).

In this paper we show how to use the canonical height on such an elliptic curve E to define a positive definite hermitian pairing on $\mathcal{E}(L)$, which in turn endows $\mathcal{E}(L)$ with the structure of a complex inner product (or unitary) space.

Theorem 1. *$E(L)/E_{\mathrm{tors}}(L)$ embeds injectively into $\mathcal{E}(L)$. The canonical height extends uniquely to $\mathcal{E}(L)$; the map $Q \mapsto \sqrt{(\hat{h}(Q))}$ makes $\mathcal{E}(L)$ into a complex normed vector space.*

Proof. It is easy to see that $\mathcal{E}(L)$ and $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$ are naturally isomorphic as vector spaces over $\mathbb{R}$, and we will identify them. The Theorem now almost follows from the fact that the canonical height extends to a positive definite quadratic form on the real vector space $\mathbb{R} \otimes_{\mathbb{Z}} E(L)$. We need only show that if $\alpha \in \mathbb{C}$ and $Q \in \mathcal{E}(L)$ then

$$\hat{h}(\alpha Q) = N(\alpha)\hat{h}(Q), \tag{1}$$

where $N(\alpha) = \alpha\bar{\alpha}$ is the norm of α as a complex number.

First we show that the function $\alpha \mapsto \hat{h}(\alpha Q)$ is continuous on $\mathbb{C}$ for any fixed $Q \in \mathcal{E}(L)$. Fix an element $\omega \in \mathcal{O}$ such that ω is non-real. Write $\|Q\| = \sqrt{\hat{h}(Q)}$. Then $\|.\|$ is a real norm. Suppose $\alpha,\ \beta$ are in $\mathbb{C}$. By the triangle inequality we have

$$-\|(\alpha-\beta)Q\| \leq \|\beta Q\| - \|\alpha Q\| \leq \|(\alpha-\beta)Q\|$$

and if we write $\alpha - \beta = \epsilon_1 + \omega\epsilon_2$ where $\epsilon_1,\ \epsilon_2$ are real, then

$$|\|\beta Q\| - \|\alpha Q\|| \leq \|(\alpha-\beta)Q\| \leq |\epsilon_1|\|Q\| + |\epsilon_2|\|\omega Q\|.$$

If β tends to α then ϵ_1, ϵ_2 will tend to 0 and so $\|\beta Q\|$ tends to $\|\alpha Q\|$. We deduce that the function $\alpha \mapsto \hat{h}(\alpha Q)$ is continuous on $\mathbb{C}$.

Since K is dense in $\mathbb{C}$ it will be sufficient to prove (1) just for $\alpha \in K$, and so by "homogeneity" just for $\alpha \in \mathcal{O}$. This is simply Lemma 1 below. □

The following lemma completes the proof of the above theorem.

Lemma 1. *Suppose $\alpha \in \mathcal{O}$ and $Q \in \mathcal{E}(L)$, then*

$$\hat{h}(\alpha Q) = N(\alpha)\hat{h}(Q) \tag{2}$$

where $N(\alpha)$ denotes the norm of α.

Proof. The proof divides into two steps:

Step 1: We prove the result (2) for $\alpha \in \mathcal{O}$ and $Q \in E(L)$. We would like to thank Professor J. Silverman for his help in proving this first step. We first recall that the map $[\alpha] : E \to E$ given by $Q \mapsto \alpha Q$ has degree $N(\alpha)$ (see [4, page 103]).

Now suppose $f : E \to E$ is a non-trivial endomorphism. We use the fact that the canonical height is defined with respect to the divisor (0). Write $f^*(0) = T_1 + \ldots + T_m$, the T_j being cleary torsion points and m is the degree of f. Then

$$\begin{aligned} \hat{h}(f(Q)) &= \hat{h}_{(0)}(f(Q)) \\ &= \hat{h}_{(f^*(0))}(Q) \\ &= \hat{h}_{(T_1)+\ldots+(T_m)}(Q) \\ &= \textstyle\sum_{j=1}^{m} \hat{h}(Q - T_j) \\ &= m\hat{h}(Q) \\ &= \deg(f)\hat{h}(Q). \end{aligned} \tag{3}$$

This completes the proof of the first step.

Step 2: Suppose now that $\alpha \in \mathcal{O}$ and $Q \in \mathcal{E}(L)$; we want to prove (2). Suppose that $Q_1, \dots, Q_n$ is a $\mathbb{Z}$-basis for the free part of $E(L)$. Then we may write $Q = \sum u_j Q_j$ where the u_j are real numbers. Thus

$$\hat{h}(\alpha Q) = \hat{h}(\sum u_j \alpha Q_j) = \mathbf{u}\mathcal{H}(\alpha Q_1, \dots, \alpha Q_n)\mathbf{u}^t \tag{4}$$

where $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathcal{H}$ denotes the height pairing matrix (see [3, page 233]). The entries of the height pairing matrix appearing in (4) are of the form

$$\begin{array}{rcl} \langle \alpha Q_i, \alpha Q_j \rangle & = & \frac{1}{2}(\hat{h}(\alpha Q_i + \alpha Q_j) - \hat{h}(\alpha Q_i) - \hat{h}(\alpha Q_j)) \\ & = & \frac{1}{2}N(\alpha)(\hat{h}(Q_i + Q_j) - \hat{h}(Q_i) - \hat{h}(Q_j)) \\ & = & N(\alpha)\langle Q_i, Q_j \rangle \end{array} \tag{5}$$

where here we have used the first step. Hence

$$\hat{h}(\alpha Q) = N(\alpha)\mathbf{u}\mathcal{H}(Q_1, \dots Q_n)\mathbf{u}^t = N(\alpha)\hat{h}(Q)$$

This completes the proof. □

We are now ready to construct our new height pairing: define, for any $Q_1,\ Q_2 \in \mathcal{E}(L)$

$$\langle Q_1, Q_2 \rangle_{\mathbb{C}} = \frac{1}{4}\sum_{r=0}^{3} \frac{1}{i^r}\hat{h}(Q_1 + i^r Q_2)$$

Theorem 2. *The above pairing makes $\mathcal{E}(L)$ into a complex inner product spaces.*

Proof. This is the standard construction of a complex inner product from a norm which satisfies the parallelogram law (see for example [2, page 237]). □

Theorem 3. *Suppose $Q_1, \dots, Q_r \in E(L)$. Define the height pairing matrix of $Q_1, \dots, Q_r$ by $\mathcal{H}_{\mathbb{C}} = (\langle Q_j, Q_k \rangle_{\mathbb{C}})_{1 \le j,k \le r}$. Then $\mathcal{H}_{\mathbb{C}}$ is a hermitian matrix. $Q_1, \dots, Q_r$ are independent over $\mathcal{O}$ if and only if $\det(\mathcal{H}_{\mathbb{C}})$ is non-zero.*

Proof. If some non-trivial $\mathcal{O}$-linear combination of the points is zero then it is straightforward to show that the rows of $\mathcal{H}_{\mathbb{C}}$ are dependent, and the result follows.

Conversely, suppose that the determinant of $\mathcal{H}_{\mathbb{C}}$ is zero. Thus the rows are dependent over $\mathbb{C}$ and so there exists complex numbers $\alpha_1, \dots, \alpha_r$, not all zero, such that $\sum \alpha_j \langle Q_j, Q_k \rangle_{\mathbb{C}} = 0$ for all k. It is easy to show that $\langle \sum \alpha_j Q_j, \sum \alpha_j Q_j \rangle = 0$. Hence $\sum \alpha_j Q_j = 0$ in $\mathcal{E}(\mathbb{C})$. Let ω be non-real element of $\mathcal{O}$; then we may write $\alpha_j = a_j + b_j\omega$ where the a_j, b_j are real. Hence $\sum a_j Q_j + \sum b_j \omega Q_j = 0$. Since $Q_j, \omega Q_j$ are all elements of $E(L)$ it follows from the well-known properties of the canonical height that some non-trivial $\mathbb{Z}$-linear combination of $Q_j, \omega Q_j$ is zero. Hence $Q_1, \dots, Q_r$ are dependent over $\mathcal{O}$. □

References

[1] J.W.S. Cassels, *Lectures on Elliptic Curves*, LMS Students Text 24, Cambridge University Press, 1991.

[2] H. G. Heuser, *Functional Analysis*, John Wiley, 1982.

[3] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.

[4] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, 1994.

[5] J. H. Silverman, *The Difference between the Weil Height and the Canonical Height on Elliptic Curves*, Math. Comp. **55** (1990), 723–743.

[6] S. Siksek, *Infinite Descent on Elliptic Curves*, Rocky Mountain Journal of Mathematics **25** (1995), 1501–1538.

Department of Mathematics, King Khalid University, Abha, PO Box 157, Saudi Arabia