LOCAL HEIGHTS ON ELLIPTIC CURVES AND INTERSECTION MULTIPLICITIES

VINCENZ BUSCH, JAN STEFFEN MÜLLER

Abstract. In this short note we prove a formula for local heights on elliptic curves over number fields in terms of intersection theory on a regular model over the ring of integers.

1. Introduction

Let K be a number field and let E be an elliptic curve in Weierstraß form defined over K. Let M_K denote the set of places on K, normalized to satisfy the product formula. For each $v \in M_K$ we denote the completion of K at v by K_v and we let $n_v = [K_v : \mathbb{Q}_v]$ be the local degree at v. Then there are certain functions $\lambda_v : E(K_v) \to \mathbb{R}$, called *local heights*, such that the canonical height $\hat{h}$ on E can be decomposed as

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

In Section 2 we discuss our normalization of the local height.

Let R be the ring of integers of K and let $\mathcal{C}$ be the minimal regular model of E over $\operatorname{Spec}(R)$. If $Q \in E(K)$, we let $\mathbf{Q} \in \operatorname{Div}(\mathcal{C})$ denote the closure of $(Q) \in \operatorname{Div}(E)(K)$ and extend this to the group $\operatorname{Div}(E)(K)$ of K-rational divisors on E by linearity.

For any non-archimedean v and any divisor $D \in \operatorname{Div}(E)(K)$ of degree zero, Lemma 4 guarantees the existence of a v-vertical $\mathbb{Q}$-divisor $\Phi_v(D)$ on $\mathcal{C}$ such that

$$(\mathbf{D} + \Phi_v(D) \,.\, F)_v = 0 \quad \text{for any } v\text{-vertical } \mathbb{Q}\text{-divisor } F \text{ on } \mathcal{C}, \tag{2}$$

where $(\cdot\,.\,\cdot)_v$ denotes the intersection multiplicity on $\mathcal{C}$ above v.

In Section 4 we will prove the following result, which is a local analogue of the classical Theorem 5.

Theorem 1. *Let v be a non-archimedean place of K and $P \in E(K) \setminus \{O\}$. Suppose that E is given by a Weierstraß equation that is minimal at v. Then we have*

$$\lambda_v(P) = 2\,(\boldsymbol{P} \,.\, \boldsymbol{O})_v - (\Phi_v((P)-(O)) \,.\, \boldsymbol{P} - \boldsymbol{O})_v\,,$$

where $\Phi_v((P)-(O))$ is any vertical $\mathbb{Q}$-divisor such that (2) holds for $D = (P)-(O)$.

Date: November 13, 2012.

Key words and phrases. Heights; elliptic curves; Arakelov theory.

Theorem 1 gives a finite closed formula for the local height that is independent of the reduction type of E at v. We hope that we can generalize Theorem 1 as described in Section 5.

The first author would like to thank the hospitality of the University of Bayreuth, where most of the research for this paper was done. We thank the anonymous referee for spotting several problems in the proof of Theorem 1.

2. Local heights

For each non-archimedean place v we let $v : K_v \longrightarrow \mathbb{Z} \cup \{\infty\}$ denote the surjective discrete valuation corresponding to v and we denote the ring of integers of K_v by $\mathcal{O}_v$.

If A is an abelian variety defined over K and D is an ample symmetric divisor on A, one can define the canonical height (or Néron-Tate height) $\hat{h}_D$ on A with respect to D. In the case of an elliptic curve $A = E$ in Weierstraß form we use the canonical height $\hat{h} = \hat{h}_{2(O)}$ with respect to the divisor $2(O)$, where O is the origin of E.

For each place v of K there is a local height (or Néron function) $\lambda_{D,v} : A(K_v) \to \mathbb{R}$, uniquely defined up to a constant, such that $\hat{h}_D$ can be expressed as a sum of local heights as in (1), see [4]. For an account of the different normalizations of the local height see [2, §4]; our normalization will correspond to the one used there, so in particular we have

$$\lambda_v(P) = 2\lambda_v^{\mathrm{SilB}}(P) + \frac{1}{6}\log|\Delta|_v \tag{3}$$

where $\lambda_v^{\mathrm{SilB}}$ is the normalization of the local height with respect to $D = (O)$ used in Silverman's second book [8, Chapter VI] on elliptic curves.

If v is an archimedean place, then we have a classical characterization of the local height. It suffices to discuss the case $K_v = \mathbb{C}$; here we consider the local height $\lambda' := \lambda_v^{\mathrm{SilB}}$ on $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}$, where $\mathrm{Im}(\tau) > 0$. We set $q = \exp(2\pi i\tau)$ and denote by

$$B_2(T) = T^2 - T + \frac{1}{6}$$

the second Bernoulli polynomial. If $P \in E(\mathbb{C}) \setminus \{O\}$, then we have

$$\lambda'(P) = -\frac{1}{2}B_2\left(\frac{\mathrm{Im}z}{\mathrm{Im}\tau}\right)\log|q| - \log|1-q| - \sum_{n\geq 1}\log|(1-q^nu)(1-q^nu^{-1})|$$

for any complex uniformisation z of P and $u = \exp(2\pi iz)$. This is [8, Theorem VI.3.4] and the following result is [8, Corollary VI.3.3]:

Proposition 2. *For all $P, Q \in E(\mathbb{C})$ such that $P, Q, P \pm Q \neq O$ we have*

$$\lambda'(P+Q) + \lambda'(P-Q) = 2\lambda'(P) + 2\lambda'(Q) - \log|x(P) - x(Q)| + \frac{1}{6}\log|\Delta|.$$

If v is a non-archimedean place we use a Theorem due to Néron which concerns the interplay of the local height λ_v and the Néron model $\mathcal{E}$ of E over $\mathrm{Spec}(\mathcal{O}_v)$. Recall that $\mathcal{E}$ can be obtained by discarding all non-smooth points from $\mathcal{C} \times \mathrm{Spec}(\mathcal{O}_v)$. Let $(\cdot\,\cdot)_v$ denote the intersection multiplicity on $\mathcal{C} \times \mathrm{Spec}(\mathcal{O}_v)$.

Let $\mathcal{E}_v$ denote the special fiber of $\mathcal{E}$ above v; then $\mathcal{E}_v$ has components $\mathcal{E}_v^0, \dots \mathcal{E}_v^r$, where r is a nonnegative integer and $\mathcal{E}_v^0$ is the connected component of the identity.

For a prime divisor $D \in \mathrm{Div}(E)(K_v)$ we write its closure in $\mathcal{E}$ as $\mathbf{D}$ and we extend this operation to $\mathrm{Div}(E)(K_v)$ by linearity. The following proposition is a special case of [4, Theorem 5.1]:

Proposition 3. *(Néron) Let $D \in \mathrm{Div}(E)(K_v)$ and let $\lambda_{D,v}$ be a local height with divisor D. For each component $\mathcal{E}_v^j$ there is a constant $\gamma_{j,v}(D)$ such that for all $P \in E(K_v) \setminus \mathrm{supp}(D)$ mapping into $\mathcal{E}_v^j$ we have*

$$\lambda_{D,v}(P) = (\boldsymbol{D} \,.\, \boldsymbol{P})_v + \gamma_{j,v}(D).$$

3. Arithmetic intersection theory

In this section we briefly recall some basic notions of Arakelov theory on $\mathcal{C}$ and its relation to canonical heights, following essentially [5].

There exists an intersection pairing

$$(\cdot \,.\, \cdot) : \mathrm{Div}(\mathcal{C}) \times \mathrm{Div}(\mathcal{C}) \to \mathbb{R},$$

called the *Arakelov intersection pairing*, which, for $D, D' \in \mathrm{Div}(\mathcal{C})$ without common component decomposes into

$$(D \,.\, D') = \sum_{v \in M_K} (D \,.\, D')_v.$$

In the non-archimedean case $(D \,.\, D')_v$ is the usual intersection multiplicity on $\mathcal{C}$ above v (defined, for example in [5, III,§2]). If v is archimedean, let $g_{D,v}$ denote a *Green's function* with respect to $D \times_v \mathbb{C}$ on the Riemann surface $E_v(\mathbb{C})$ (see [5, II,§1]). Then $(D \,.\, D')_v$ is given by $g_{D,v}(D') := \sum_i n_i g_{D,v}(Q_i)$ if $D' \times_v \mathbb{C} = \sum_i n_i Q_i$. See [5, IV,§1].

Let $v \in M_K$ be non-archimedean. We say that a divisor F on $\mathcal{C}$ is *v-vertical* if $\mathrm{supp}(F) \subset \mathcal{C}_v$ and we denote the subgroup of such divisors by $\mathrm{Div}_v(\mathcal{C})$. We also need to use elements of the group $\mathbb{Q} \otimes \mathrm{Div}_v(\mathcal{C})$ of v-vertical $\mathbb{Q}$-divisors on $\mathcal{C}$.

We define the operation $D \to \mathbf{D}$ on $\mathrm{Div}(E)(K)$ as in Section 2.

Lemma 4. *(Hriljac) For all $D \in \mathrm{Div}(E)(K)$ of degree zero, there exists $\Phi_v(D) \in \mathbb{Q} \otimes \mathrm{Div}_v(\mathcal{C})$, unique up to rational multiples of $\mathcal{C}_v$, such that we have*

$$(\boldsymbol{D} + \Phi_v(D) \,.\, F)_v = 0$$

for any $F \in \mathbb{Q} \otimes \mathrm{Div}_v(\mathcal{C})$.

Proof: See for instance [5, Theorem III.3.6]. □

Note that we can pick $\Phi_v(D) = 0$ if $\mathcal{C}_v$ has only one component. This holds for all but finitely many v.

In analogy with a result for elliptic surfaces due to Manin (cf. [8, Theorem III.9.3]), the following theorem relates the Arakelov intersection to the canonical height. See [5, III,§5] for a proof.

Theorem 5. *(Faltings, Hriljac) Let $D, D' \in \mathrm{Div}(E)(K)$ have degree zero and satisfy $[D] = [D'] = P \in \mathrm{Jac}(E)(K) = E(K)$. For each non-archimedean v such that $\mathcal{C}_v$ has more than one component choose some $\Phi_v(D)$ as in Lemma 4 and set $\Phi(D) = \sum_v \Phi_v(D)$. Then we have*

$$(\boldsymbol{D} + \Phi(D) \,.\, \boldsymbol{D'}) = -\hat{h}(P).$$

4. Proof of the Main Theorem

For a non-archimedean place v we let $E^0(K_v)$ denote the subgroup of points of $E(K_v)$ mapping into the connected component of the identity of the special fiber $\mathcal{E}_v$ of the Néron model of E over $\mathrm{Spec}(\mathcal{O}_v)$. We write $\gamma_{j,v}$ for the constant $\gamma_{j,v}(2(O))$ introduced in Proposition 3 with respect to our local height λ_v. It is easy to see that our normalization corresponds to the choice $\gamma_{0,v} = 0$; therefore we have

$$\lambda_v(P) = (2\mathbf{O}.\mathbf{P})_v = 2(\mathbf{P}.\mathbf{O})_v. \tag{4}$$

for any $P \in E^0(K_v) \setminus \{O\}$. Because P and O reduce to the same component, we also have $\Phi_v((P) - (O)) = 0$ which proves the theorem for such points.

Next we want to find the constants $\gamma_{j,v}$ for $j > 0$. We will first compare the local height with Arakelov intersections for archimedean places.

Lemma 6. *Let v be an archimedean place. The local height $\lambda_v^{\mathrm{SilB}}$ is a Green's function with respect to $D = (O)$ and the canonical volume form on the Riemann surface $E_v(\mathbb{C})$. Hence the function*

$$g_{P,v}(Q) := \lambda_v^{\mathrm{SilB}}(Q - P)$$

is a Green's function with respect to the divisor (P) for any $P \in E_v(\mathbb{C})$.

For a proof see [5, Theorem II.5.1]. We extend this by linearity to get a Green's function $g_{D,v}$ with respect to any $D \in \mathrm{Div}(E_v)(\mathbb{C})$.

Lemma 7. *Let v be an archimedean place of K. For all $P \in E_v(\mathbb{C}) \setminus \{O\}$ and $Q \in E_v(\mathbb{C}) \setminus \{\pm P, O\}$ we have*

$$g_{D,v}(D_Q) = -\lambda_v(P) - \log|x(P) - x(Q)|_v,$$

where $D = (P) - (O)$ and $D_Q = (P + Q) - (Q)$.

Proof: We have

$$\begin{aligned} g_{D,v}(D_Q) &= g_{P+Q,v}(P) - g_{P+Q,v}(O) - g_{Q,v}(P) + g_{Q,v}(O) \\ &= 2\lambda'(Q) - \lambda'(P+Q) - \lambda'(P-Q), \end{aligned}$$

where $\lambda' = \lambda_v^{\mathrm{SilB}}$ and the second equality follows from Lemma 6. However, by Proposition 2 we have

$$2\lambda'(Q) - \lambda'(P+Q) - \lambda'(P-Q) = -2\lambda'(P) + \log|x(P) - x(Q)|_v - \frac{1}{6}\log|\Delta|_v.$$

An application of (3) finishes the proof of the lemma. □

Lemma 8. *Theorem 1 holds if for each reduction type $\mathcal{K} \notin \{I_0, I_1, II, II^*\}$ there is a prime number p and an elliptic curve $E(\mathcal{K})/\mathbb{Q}$, given by a Weierstraß equation that is minimal at p, satisfying the following conditions:*

(i) *The Néron model $\mathcal{E}(\mathcal{K})$ of $E(\mathcal{K})$ has reduction type $\mathcal{K}$ at p.*
(ii) *For each connected component $\mathcal{E}(\mathcal{K})_p^j$, there is a point $P_j \in E(\mathcal{K})(\mathbb{Q}) \setminus \{O\}$ reducing to $\mathcal{E}(\mathcal{K})_p^j$.*
(iii) *We have $v_p(x(P_0)) \geq 0$.*

Proof: Let v be a non-archimedean place of K, let k_v be the residue class field at v. Let $N_v = \frac{n_v}{\log(\#k_v)}$, where $n_v = [K_v : \mathbb{Q}_v]$. If $P \notin E^0(K_v)$, we have $v_p(x(P)) \geq 0$ and hence $(\mathbf{P} \,.\, \mathbf{O})_p = 0$ is immediate.

Now let $\mathcal{K}$ be a reduction type of E at v. Then, for any $j \in \{0, \ldots, r\}$, both $\gamma_{j,v} \cdot N_v$ and $\left(\Phi_v((P_j) - (O)) \,.\, \mathbf{P}_j - \mathbf{O}\right)_v \cdot N_v$ do not depend on K, E or v, but only on $\mathcal{K}$ and j. For the former assertion, see [2], where the values of all possible $\gamma_{j,v}$ are determined and for the latter see [1].

Therefore it suffices to show

$$\lambda_p(P_j) = \gamma_{j,p} = -\left(\Phi_p((P_j) - (O)) \,.\, \mathbf{P}_j - \mathbf{O}\right)_p \tag{5}$$

for all $j \neq 0$, where $P_j \in E(\mathcal{K})(\mathbb{Q})$ is as in (ii). We can assume $\mathcal{K} \notin \{I_0, I_1, II, II^*\}$, since for those reduction types only the connected component of the identity contains $\mathbb{Q}_p$-rational points.

Let $j \neq 0$, let $P = P_j$, let $D = (P) - (O)$ and let $D_Q = (P + Q) - (Q)$ for each $Q \in E(\mathcal{K})(\mathbb{Q})$.

From Theorem 5 we deduce

$$-\sum_p (\mathbf{D} + \Phi_p(D) \,.\, \mathbf{D_Q})_p - g_{D,\infty}(D_Q) = \sum_p \lambda_p(P) + \lambda_\infty(P)$$

for any $Q \in E(\mathcal{K})(\mathbb{Q}) \setminus \{P, -P, O\}$. For each prime p, the corresponding summand is a rational multiple of $\log p$, so together with the product formula (see [4, §2.1]) Lemma 7 implies

$$\lambda_p(P) = -(\mathbf{D} + \Phi_p(D) \,.\, \mathbf{D_Q})_p - \log |x(P) - x(Q)|_p \tag{6}$$

for all primes p, by independence of logarithms over $\mathbb{Q}$.

Now consider $Q = P_0 \in E(\mathcal{K})^0(\mathbb{Q}_p) \cap E(\mathcal{K})(\mathbb{Q}) \setminus \{O\}$ and expand

$$(\mathbf{D} \,.\, \mathbf{D_Q})_p = (\mathbf{P} \,.\, \mathbf{P{+}Q})_p - (\mathbf{P} \,.\, \mathbf{Q})_p - (\mathbf{O} \,.\, \mathbf{P{+}Q})_p + (\mathbf{O} \,.\, \mathbf{Q})_p.$$

By assumption, we have

$$(\mathbf{P} \,.\, \mathbf{Q})_p = (\mathbf{O} \,.\, \mathbf{P{+}Q})_p = 0$$

since the respective points lie on different components. Moreover, because of the Néron mapping property, (see [8, IV,§5]) translation by P extends to an automorphism of $\mathcal{E}(\mathcal{K})$, so we have

$$(\mathbf{P} \,.\, \mathbf{P{+}Q})_p = (\mathbf{O} \,.\, \mathbf{Q})_p.$$

However, it follows from the definition of the intersection pairing in [5, III,§2] that the latter vanishes by assumption (iii), since Q and O do not reduce to the same point modulo

$\mathcal{K}$	p	$E(\mathcal{K})$
I_n $n \geq 2$	$p > 3$	$y^2 = (x+1-p)(x^2 - p^{n-1}x + p^n)$
		$P_0 = (p-1, 0)$; $P_1 = (p, p)$
III	7	$y^2 = x^3 + 7x + 7^2$
		$P_0 = (-3, 1)$; $P_1 = (0, 7)$
IV	7	$y^2 = x^3 + 4 \cdot 7^2$
		$P_0 = (-3, 13)$; $P_1 = (0, 14)$
I_0^*	7	$y^2 + 7^2 y = x^3 + 7x^2 + 7^2 x$
		$P_0 = (-6, -6)$; $P_1 = (0, 0)$; $P_2 = (14, 49)$
$I_n^*, n \geq 1$ odd $n = 2k-3$	2	$y^2 + 2^k y = x \cdot (x - (2^k - 2)) \cdot (x + 2^{k+1})$
		$P_0 = (-1, 2^{k+1} - 1)$; $P_1 = (0, 0)$
$I_n^*, n \geq 2$ even $n = 2k-2$	2	$y^2 - 2^{k+1} y = x \cdot (x - (2^k - 2)) \cdot (x + 2^k)$
		$P_0 = (-1, 2^k - 1)$; $P_1 = (0, 0)$; $P_2 = (-2^k, 0)$
IV^*	7	$y^2 = x^3 + 2 \cdot 7^3 x + 7^4$
		$P_0 = (32, 239)$; $P_1 = (0, 49)$
III^*	7	$y^2 = x^3 + 7^3 x + 5 \cdot 7^5$
		$P_0 = (-38, 127)$; $P_1 = (98, 1029)$

TABLE 1. $E(\mathcal{K})$ for $\mathcal{K} \notin \{I_0, I_1, II, II^*\}$

p. Therefore we find that $(\mathbf{D} \,.\, \mathbf{D_Q})_p = 0$. Since we cannot have $v_p(x(P) - x(Q)) > 0$, the proof of (5) and hence of the Lemma follows from (6). □

In order to finish the proof of the Theorem, we only need to prove the following result:

Lemma 9. *For each reduction type $\mathcal{K} \notin \{I_0, I_1, II, II^*\}$ the elliptic curve $E(\mathcal{K})$ listed in Table 1 satisfies the conditions of Lemma 8.*

Proof: This is a straightforward check using the proof of Tate's algorithm in [8, III,§9]. If the component group $\Psi(\mathcal{K})$ of $\mathcal{E}(\mathcal{K})$ is cyclic, it suffices to list $P_1 \in E(\mathcal{K})(\mathbb{Q})$ mapping to a generator of $\Psi(\mathcal{K})$ to guarantee the existence of P_j as in Proposition 8 for all $j \neq 0$. In the remaining case I_n^*, n even, we have $\Psi(\mathcal{K}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and hence we need to list two points P_1 and P_2 mapping to generators of $\Psi(\mathcal{K})$. □

Remark 10. It is well-known that λ_v is constant on non-identity components of $\mathcal{E}_v$. This follows from Theorem 3 as above, but we are not aware of any previous result interpreting the constants $\gamma_{j,v}$ in terms of intersection theory.

Remark 11. It is easy to see that we can consider $P \in E(K_v)$ in the statement of Theorem 1. In that case, we have to look at the respective Zariski closures on $\mathcal{C} \times \mathrm{Spec}(\mathcal{O}_v)$ and observe that Lemma 4 remains correct in the local case.

Remark 12. Although Theorem 1 requires E to be given by a minimal Weierstraß equation at v, we can find the value of λ_v for other models of E using the transformation formula [2, Lemma 4].

Remark 13. According to David Holmes, Theorem 1 can also be proved by a direct comparison using Néron's original construction of the canonical height pairing. The details will appear in Holmes' forthcoming PhD thesis at the University of Warwick.

5. Outlook

It would be interesting to generalize Theorem 1 to the case of a Jacobian J of a curve C of genus $g \geq 2$. There are analogues of Proposition 3 in this situation and if we use the divisor $T = \Theta + [-1]^*\Theta$, where $\Theta \in \mathrm{Div}(J)$ is a theta divisor, then Theorem 5 also generalizes. For instance, if C is hyperelliptic with a unique K-rational point ∞ at infinity, then every $P \in J(K)$ can be represented using a divisor $D = \sum_{i=1}^{d}(P_i) - d(\infty)$, where $d \leq g$, and a natural analogue of Theorem 1 would be an expression of $\lambda_v = \lambda_{T,v}$ in terms of the intersections $(\mathbf{P}_i, \infty)$ and the vertical $\mathbb{Q}$-divisor $\Phi_v(D)$.

This would be interesting, for example, because for $g \geq 3$ it is currently impossible to write down non-archimedean local heights explicitly, as one needs to work on an explicit embedding of the Kummer variety $J/\{\pm 1\}$ into $\mathbb{P}^{2^g-1}$ and these become rather complicated as g increases. See [6, Chapter 4] for a discussion. Accordingly, the existing algorithms [3], [7] for the computation of canonical heights use the generalization of Theorem 5 directly by choosing (rather arbitrarily) divisors D_1 and D_2 that represent P. These algorithms could be simplified significantly if a generalization of Theorem 1 were known.

References

[1] D. A. Cox and S. Zucker, *Intersection numbers of sections of elliptic surfaces,* Invent. Math. **53**, 1–44 (1969).

[2] J.E. Cremona, M. Prickett and S. Siksek, *Height difference bounds on elliptic curves over number fields,* J. Number Theory **116**, 42–68 (2006).

[3] D. Holmes, *Computing Néron-Tate heights of points on hyperelliptic Jacobians*, J. Number Theory (2012), doi:10.1016/j.jnt.2012.01.002.

[4] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York, 1983.

[5] S. Lang, *Introduction to Arakelov theory*, Springer-Verlag, New York, 1988.

[6] J.S. Müller, *Computing canonical heights on Jacobians*, PhD thesis, Universität Bayreuth (2010).

[7] J.S. Müller, *Computing canonical heights using arithmetic intersection theory*, Preprint (2011). arXiv:math/1105.1719v2 [math.NT]; to appear in Math. Comp.

[8] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1995

Fachbereich Mathematik, Universität Hamburg, Bundesstrasse 55, 20146 Hamburg, Germany

E-mail address: busch@math.uni-hamburg.de

E-mail address: jan.steffen.mueller@math.uni-hamburg.de