Compositio Mathematica **122:** 299–313, 2000.

Canonical Heights on Elliptic Curves in Characteristic p

MATTHEW A. PAPANIKOLAS
Department of Mathematics, Pennsylvania State University, University Park, PA 16802 U.S.A. e-mail: map@math.psu.edu

(Received: 7 August 1998; 22 March 1999)

Abstract. Let $k = \mathbb{F}_q(t)$ be the rational function field with finite constant field and characteristic $p \geqslant 3$, and let K/k be a finite separable extension. For a fixed place v of k and an elliptic curve E/K which has ordinary reduction at all places of K extending v, we consider a canonical height pairing $\langle\ ,\ \rangle_v : E(K^{\text{sep}}) \times E(K^{\text{sep}}) \to \mathbb{C}_v^{\times}$ which is symmetric, bilinear and Galois equivariant. The pairing $\langle\ ,\ \rangle_\infty$ for the "infinite" place of k is a natural extension of the classical Néron–Tate height. For v finite, the pairing $\langle\ ,\ \rangle_v$ plays the role of global analytic p-adic heights. We further determine some hypotheses for the nondegeneracy of these pairings.

Mathematics Subject Classifications (2000). 11G05, 11G07, 11R58, 11G50.

Key words: elliptic curves, global canonical heights, Mazur–Tate sigma function, global function fields

1. Introduction

Our goal in this paper is to construct and investigate canonical heights on elliptic curves defined over global function fields in characteristic p. These heights will take values in the completions of the function field and serve as analogues of both the classical Néron–Tate height and also analytic p-adic heights on elliptic curves over number fields, cf. [3, 8, 10, 13, 14].

Except in Sections 3 and 4, we maintain the following notation throughout the paper. We take p to be an odd prime; $\mathbb{F}_q$ the finite field with $q = p^n$ elements; k the rational function field $\mathbb{F}_q(t)$; and A the polynomial ring $\mathbb{F}_q[t]$. The valuations of the field k corresponding to maximal ideals of A are called *finite places*; the unique remaining place is the *infinite* place, denoted ∞, with $\text{ord}_\infty = -\deg$, where deg is the degree map on polynomials extended to rational functions.

We let K/k denote a *global function field*, i.e., a finite separable field extension of k, and we let $\mathcal{O}$ be the integral closure of A in K. For a place w of K, we let K_w denote the completion at w; $\mathcal{O}_w$ its valuation ring; $\mathbb{F}_w$ its residue field; and $\mathbb{C}_w$ the completion of an algebraic closure of K_w. Furthermore, $U^1(K_w)$ and $U^1(\mathbb{C}_w)$ are the groups of 1-units. A place of K is either finite or infinite depending on the place it extends from k. Finally, for any field F, we let F^{sep} be a separable closure and $\overline{F}$ an algebraic closure.

For a fixed place v of k, we consider an elliptic curve E/K which has *ordinary reduction* at all places of K extending v. That is, the formal group of each reduced curve has height 1. In Section 5 we define a Galois equivariant quadratic form $\widehat{H}_v: E(K^{\text{sep}}) \to \mathbb{C}_v^{\times}$, which equivalently induces a symmetric bilinear pairing,

$$\langle\ ,\ \rangle_v: E(K^{\text{sep}}) \times E(K^{\text{sep}}) \to \mathbb{C}_v^{\times}.$$

We construct $\widehat{H}_v$ as a product of local factors. At the places not dividing v, these local factors are derived from intersection multiplicities on the Néron model for E/K, and at the places above v, the local heights are defined using the Mazur–Tate sigma function [9].

It should be noted that these constructions contain differences depending on whether v is a finite or infinite place of k. We find in Section 6 that for $v = \infty$, the resulting ∞-adic height extends the Néron–Tate height. Indeed we find for all $P \in E(K^{\text{sep}})$ that $\deg(\widehat{H}_\infty(P)) = 2\hat{h}_{\text{NT}}(P)$. If v is a finite place, the v-adic height takes values in $U^1(\mathbb{C}_v)$. In Sections 7 and 8 we investigate the nondegeneracy of these height functions. Just as for p-adic heights for elliptic curves defined over number fields, the nondegeneracy of the v-adic height is related to the nonexistence of universal norms coming from the so-called Carlitz cyclotomic tower of K (see [11, 12]).

The assumption that p is odd is not necessary, but for the purposes of length we have disregarded the case where $p = 2$. Moreover, the flavor of the results are identical [12].

Finally, it is important to remark that the canonical heights discussed in this paper are effectively computable, and in Section 9 we discuss an explicit example.

2. Elliptic Curves over Global Function Fields

Fixing a field K/k which is the function field of a smooth curve $X/\mathbb{F}_q$, we let E/K be an elliptic curve defined over K and take $\mathcal{E}/X$ to be a Néron model for E/K with identity component $\mathcal{E}^0/X$. Using the intersection multiplicities of sections on $\mathcal{E}$, it is possible to construct the classical *Néron–Tate canonical height pairing,*

$$\langle\ ,\ \rangle_{\text{NT}}: E(K^{\text{sep}}) \times E(K^{\text{sep}}) \to \mathbb{Q},$$

which is symmetric and bilinear and when restricted to $E(K)$ is nondegenerate modulo torsion [16]. Equivalently, we can construct the associated quadratic form $\hat{h}_{\text{NT}}$, which we define so that $\hat{h}_{\text{NT}}(P) = \frac{1}{2}\langle P, P\rangle_{\text{NT}}$. We note that here the Néron–Tate height is normalized to take values which are independent of the chosen field of definition.

As is well known, the Néron–Tate height can be computed as a sum of local heights (see [7, 16]). We fix a Weierstrass equation for E,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K. \tag{2.1}$$

For a place w of K, we let $E_0(K_w) \subset E(K_w)$ denote the subgroup of points whose

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

reduction is nonsingular at w, i.e., the points whose sections meet $\mathcal{E}^0$ on the fiber above w. There is a local height function, $\lambda_w: E_0(K_w) \to \mathbb{Z}$, defined so that for $P \in \mathcal{E}^0(X) \subset E(K)$, the Néron–Tate height is obtained by the formula

$$\hat{h}_{\mathrm{NT}}(P) = \frac{1}{2[K:k]} \sum_{w \in X} [\mathbb{F}_w : \mathbb{F}_q] \lambda_w(P). \tag{2.2}$$

If $P \in \mathcal{E}^0(X)$ and (2.1) is minimal at w, then λ_w is defined by $\lambda_w(P) = \max\{-\mathrm{ord}_w(x(P)), 0\}$.

3. The Mazur–Tate Sigma Function

Here we review some facts about the Mazur–Tate sigma function as defined in [9]. This function, defined on the formal group of an elliptic curve over a local field, is a natural non-Archimedean analogue of the classical Weierstrass sigma function, and similar to the classical sigma function, it provides an analytic local height function on an elliptic curve. For more details on its connection with p-adic heights for elliptic curves over number fields see [10]. There is also an analogue of the Weierstrass zeta function, defined by Voloch [19], which is also of interest here.

Throughout this section and the next we diverge from the previous notation and maintain the following conventions: K is a field complete with respect to a discrete valuation ord; $\mathcal{O}$ is the valuation ring of K; and $\mathbb{F}$ is its residue field. We assume that both $\mathcal{O}$ and $\mathbb{F}$ have characteristic p and begin with some necessary definitions.

Let E/K be an elliptic curve with ordinary reduction, and fix an invariant differential ω on E. We choose a minimal Weierstrass equation (2.1) so that $\omega = dx/(2y + a_1 x + a_3)$. Taking $\widehat{E}/\mathcal{O}$ for the formal completion of the Néron model of E along its zero-section, we then pick a uniformizing parameter z on $\widehat{E}$ and let $\beta = (\omega/dz)(O)$. The multiplication-by-p map on $\widehat{E}$ then has the form

$$[p](z) = \alpha\beta^{p-1} z^p + \cdots, \quad \in \mathcal{O}[\![z^p]\!], \tag{3.1}$$

where α is the *Hasse invariant* of E/K (see §12.4 of [6]).

The fraction field L of the power series ring $\mathcal{O}[\![z]\!]$ is naturally considered the field of rational functions on $\widehat{E}$, and it contains $K(E)$ as a subfield. For an integer m, the mth *division polynomial with respect to* ω is the function $f_m \in K(E) \subset L$ with divisor $[m]^{-1}(O) - m^2(O)$ such that

$$\frac{z^{m^2} f_m(z)}{[m](z)}(O) = \beta^{1-m^2},$$

as defined in [9]. Such division polynomials satisfy many recursion formulas and possess a rich structure. Notably,

$$f_{p^n}(z) = f_{p^{n-1}}([p](z)) f_p(z)^{p^{2n-2}}. \tag{3.2}$$

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

THEOREM 3.3 (Mazur–Tate [9]). *The sigma function $\sigma = \sigma_{E,\omega}$ is characterized as the unique function in $\beta z(1 + z\mathcal{O}[\![z]\!])$ satisfying any one of the following equivalent properties.*

(a) *If P, Q are nonzero points in $\widehat{E}(\mathcal{O})$, then*

$$\frac{\sigma(P-Q)\sigma(P+Q)}{\sigma(P)^2\sigma(Q)^2} = x(Q) - x(P).$$

(b) *If $m \in \mathbb{Z}$ and $Q \in \widehat{E}(\overline{\mathcal{O}})$, then*

$$\sigma(mQ) = \sigma(Q)^{m^2} f_m(Q),$$

*where f_m is the m*th *division polynomial with respect to ω.*

(c) *If $Q \in \widehat{E}(\mathcal{O})$, then*

$$\sigma(pQ) = \sigma(Q)^{p^2} f_p(Q).$$

4. A Formula for the Sigma Function

Recalling (3.1), we deduce that $[p^n](z) = \alpha_n \beta^{p^n-1} z^{p^n} + \cdots \in \mathcal{O}[\![z^{p^n}]\!]$, where $\alpha_n = \alpha \cdot \alpha^p \cdot \alpha^{p^2} \cdot \cdots \cdot \alpha^{p^{n-1}} = \alpha^{(p^n-1)/(p-1)}$. An exercise in formal power series shows that inverting $[p^n](z)$ with respect to composition yields

$$[p^n]^{-1}(z) = \frac{1}{\beta}\left(\frac{\beta}{\alpha_n}\right)^{1/p^n} z^{1/p^n} + \cdots \quad \in \mathcal{O}^{1/p^n}[\![z^{1/p^n}]\!], \tag{4.1}$$

which when raised to the p^nth power results in a series in $\mathcal{O}[\![z]\!]$. This series will converge for points in the formal group, which highlights the fact that the points in $\widehat{E}$ are uniquely p-divisible since $\widehat{E}$ has height 1.

THEOREM 4.2. *Let $\sigma(z)$ be the power series given by the infinite product*

$$\sigma(z) = \beta z \prod_{n \geqslant 1} \left[\frac{\beta^{p-1}}{\alpha^{p^{n-1}} \alpha_n^{p-1}} z^{p-1} f_p([p^n]^{-1}(z))^{p^{n-1}} \right]^{p^{n-1}}.$$

The product converges in $\mathcal{O}[\![z]\!]$ and the resulting series is the Mazur–Tate sigma function $\sigma_{E,\omega}$.

Proof. For convergence, it suffices to show that each factor in the square brackets above is a 1-unit in $\mathcal{O}[\![z]\!]$, which follows from (4.1). A straightforward manipulation of the factors permits us to prove that $\sigma(z)$ satisfies the identity in (3.3c) and thus represents the sigma function. See [12] for further details. □

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

5. Canonical Heights

We return to the notation given in Sections 1 and 2. For a global function field K/k, let E/K be an elliptic curve with ordinary reduction at all places of K which extend a chosen place v of k. In this section we construct a symmetric bilinear pairing

$$\langle\ ,\ \rangle_v : E(K) \times E(K) \to \mathbb{C}_v^\times, \tag{5.1}$$

which will serve as a canonical height. Our interests will lie with investigating various properties of these heights as well with determining their nondegeneracy (see Sections 7 and 8). Although the constructions are similar, the resulting pairing will have a different meaning depending on whether the preferred place v is finite or infinite. The ∞-adic height plays the role of the Néron–Tate height (see Theorem 6.1) and the v-adic height (v finite) is the analogue of the analytic p-adic heights for elliptic curves over number fields, cf. [8, 10, 14].

The techniques in this section are fairly standard, so we merely address the important points. Moreover, our construction is similar to that of [10]; for more details the reader is directed to [12]. For each place v of k we fix a uniformizer π_v in $\mathbb{F}_v k$, and we observe that the group $\pi_v^{\mathbb{Q}} \cdot U^1(\mathbb{C}_v)$ is uniquely divisible. For $x \in \mathbb{C}_v^\times$, we let $\langle x \rangle = \langle x \rangle_v$ denote the *positive part* of x, i.e., the class of x in $\pi_v^{\mathbb{Q}} \cdot U^1(\mathbb{C}_v)$ modulo $\overline{\mathbb{F}}_v^\times$. The values of our heights will be taken in the positive elements of $\mathbb{C}_v^\times$.

We then fix a Weierstrass equation for E/K as in (2.1) and let $\omega = dx/(2y + a_1 x + a_3)$. For each place w of K, we let z_w be a local uniformizing parameter for $\widehat{E}/\mathcal{O}_w$ and $\beta_w = (\omega/dz_w)(O) \in K_w^\times$. We consider the subgroup $E_v(K) \subset E(K)$ of finite index consisting of points on the identity component $\mathcal{E}^0$ of $\mathcal{E}$ which also specialize to O on the fibers of places which extend v, i.e.,

$$E_v(K) = \mathcal{E}^0(X) \cap \bigcap_{w|v} \widehat{E}(\mathcal{O}_w).$$

For each $P \in E_v(K) \setminus \{O\}$, we define an idele $i(P) \in \mathbf{A}_K^\times$ component-wise as follows:

$$i(P)_w = \begin{cases} 1 & \text{if } w \mid \infty \text{ and } v \neq \infty, \\ \beta_w & \text{if } w \nmid v \text{ finite and } P \notin \widehat{E}\,(\mathcal{O}_w), \\ \beta_w z_w(P) & \text{if } w \nmid v \text{ finite and } P \in \widehat{E}\,(\mathcal{O}_w), \\ \sigma_{E/K_w,\omega}(P) & \text{if } w \mid v. \end{cases} \tag{5.2}$$

We set $i(O) = 1$. We observe that if v is finite then $i(P)$ is supported away from ∞. Furthermore, we find that for $w \nmid v$ or ∞,

$$\operatorname{ord}_w(i(P)_w) = \tfrac{1}{2}\lambda_w(P). \tag{5.3}$$

We then define a map $\rho_v^K : \mathbf{A}_K^\times \to \mathbb{C}_v^\times$ as follows. We take

$$\rho_v^K((e_w)_w) = \rho_v^k\big(\mathbf{N}_k^K (e_w)_w\big)^{1/[K:k]}, \tag{5.4}$$

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

where $\mathbf{N}_k^K$ is the norm map on ideles and

$$\rho_v^k((e_{\tilde{v}})_{\tilde{v}}) = \frac{1}{\langle e_v \rangle} \prod_{\tilde{v} \neq \infty} \pi_{\tilde{v}}^{\mathrm{ord}_{\tilde{v}}(e_{\tilde{v}})},$$

for $\pi_{\tilde{v}}$ the positive uniformizer of $\tilde{v}$ in $\mathbb{F}_v A$. Note that the values of ρ_∞^k are in $\pi_\infty^{\mathbb{Q}} \cdot U^1(\mathbb{C}_\infty)$, whereas for v finite, ρ_v^k takes values in $U^1(\mathbb{C}_v)$.

By combining (5.2) and (5.4), we define a height function by

$$\widehat{H}_v = \rho_v^K \circ i^2 \colon E_v(K) \to \mathbb{C}_v^\times,$$

which is a quadratic form and hence a 'canonical height'. We observe that the values of $\widehat{H}_v$ are independent of the choices of formal parameters and differentials made in (5.2). Because the image is contained in a uniquely divisible subgroup of $\mathbb{C}_v^\times$, we can extend the definition to all of $E(K)$. The following proposition summarizes the above discussion.

PROPOSITION 5.5. *Let K/k be a global function field and E/K an elliptic curve with ordinary reduction at all the places of K extending v. There is a unique quadratic form $\widehat{H}_v \colon E(K) \to \mathbb{C}_v^\times$ which extends*

$$\widehat{H}_v = \rho_v^K \circ i^2 \colon E_v(K) \to \mathbb{C}_v^\times.$$

Furthermore, the height behaves well under base-extension, and gives rise to a symmetric, bilinear pairing

$$\langle\ ,\ \rangle_v \colon E(K^{\mathrm{sep}}) \times E(K^{\mathrm{sep}}) \to \mathbb{C}_v^\times,$$

with $\widehat{H}_v(P) = \langle P, P \rangle_v$, which is Galois equivariant, i.e., $\langle \tau P, \tau Q \rangle_v = \langle P, Q \rangle_v$ for all $P, Q \in E(K^{\mathrm{sep}})$ and all $\tau \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$.

6. Extension of the Néron–Tate Height

In this section, we will prove the following theorem which shows that the ∞-adic height as defined in the previous section actually extends the Néron–Tate height in a natural way.

THEOREM 6.1. *Let E/K be an elliptic curve with ordinary reduction at all the infinite places of K. Then for all $P, Q \in E(K^{\mathrm{sep}})$,*

$$\deg(\langle P, Q \rangle_\infty) = \langle P, Q \rangle_{\mathrm{NT}},$$

where here $\deg = -\mathrm{ord}_\infty$.

Proof. Because the value of $\widehat{H}_\infty$ is independent of a chosen Weierstrass equation, we are free to fix a Weierstrass equation which is minimal at all places of K extending ∞. Furthermore, it suffices that the theorem holds on $E_\infty(K)$. Given

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

the ways we have normalized our pairings, we need to show that

$$\deg(\widehat{H}_\infty(P)) = 2\,\hat{h}_{\mathrm{NT}}(P). \tag{6.2}$$

By the definition of $\widehat{H}_\infty$ along with (5.3) and (5.4), we have

$$\widehat{H}_\infty(P)^{[K:k]} = \prod_{w|\infty} \left\langle \mathbf{N}_{k_\infty}^{K_w} \sigma_{E/K_w,\omega}(P)^{-2} \right\rangle \prod_{v\neq\infty} \prod_{w|v} \pi_v^{[\mathbb{F}_w:\mathbb{F}_v]\lambda_w(P)},$$

and thus the terms from (6.2) corresponding to the finite places exactly match those from (2.2). Finally we need to show for each $w \mid \infty$ that, before taking norms, we have $\mathrm{ord}_w(\sigma_{E/K_w,\omega}(P)^2) = \lambda_w(P)$, which follows from (3.3) and the ultrametric inequality. □

7. Nondegeneracy of v-Adic Heights

A symmetric bilinear pairing of Abelian groups $E \times E \to G$ with G uniquely divisible is said to be *nondegenerate* if the kernel consists only of the torsion elements of E. Theorem 6.1 assures us that the ∞-adic height pairing is nondegenerate on $E(K)$.

On the other hand, the values of the v-adic pairing (for v a finite place of k) are 1-units in $\mathbb{C}_v$, and so *a priori* we can say little about the nondegeneracy of these heights. In this section and the next we investigate conditions for the nondegeneracy of the pairing $\langle\ ,\ \rangle_v$ on $E(K)$, and we find that, for E/k defined over the rational function field, nondegeneracy on $E(K)$ can be proven in many general cases. Additionally, in the next section we show that the induced pairing

$$\langle\ ,\ \rangle_v : (E(K) \otimes \mathbb{Z}_p) \times (E(K) \otimes \mathbb{Z}_p) \to \mathbb{C}_v^\times,$$

is also nondegenerate under these same hypotheses.

Remark 7.1. By contrast, for analytic p-adic height pairings for elliptic curves defined over number fields [8, 14], it is a difficult problem to determine nondegeneracy (see [15]), and it is not known in general when such pairings are nondegenerate.

For this section and the next we restrict ourselves to the following situation: E/k is an elliptic curve defined over the rational function field with ordinary reduction at both v and ∞. This reduction assumption is quite weak, since if E is not supersingular, then all but finitely many places will have ordinary reduction. We will further fix a Weierstrass equation (2.1) which is minimal at both v and ∞.

Let K/k be a global function field. If v (resp. ∞) ramifies in K, then we will also assume that E has good reduction at v (resp. ∞). This assumption ensures that our chosen equation is minimal at all places above v and ∞ in K.

For a point $P \in E_v(K) \cap E_\infty(K)$ and a fixed positive integer N, we take $V_N : E^{(p^N)} \to E$ to be the Verschiebung (the dual of the p^Nth power Frobenius

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

morphism), and we define

$$V_N^{-1}(P) \subset E^{(p^N)}(k^{\text{sep}})$$

to be the inverse image of the point P under V_N, which consists of p^N distinct points.

Let w denote a place of K above either v or ∞. If $P \in E_v(K) \cap E_\infty(K)$, then because the formal group $\widehat{E}^{(p^N)}/\mathcal{O}_w$ has height 1, there is a unique point,

$$Q_w = Q_w(P) = Q_{w,N}(P) \in V_N^{-1}(P), \tag{7.2}$$

such that $Q_w \in \widehat{E}^{(p^N)}(\mathcal{O}_w)$. For different places w and w' (either both extending v or both extending ∞), the points Q_w and $Q_{w'}$ are related. Indeed, if we fix a separable closure k_v^{sep} so that

$$k_v \subset K_w \subset k_v^{\text{sep}},$$

we see that the absolute value of w' on K is obtained through an embedding $\tau: K \hookrightarrow k_v^{\text{sep}}$, which induces an embedding $\tau: K_{w'} \hookrightarrow k_v^{\text{sep}}$. For such an embedding τ, we then have $\tau Q_{w'}(P) = Q_w(\tau P)$.

We now introduce a hypothesis which will play a crucial role in the proof of Theorem 7.4, the main theorem of this section. In Section 8 we will investigate the generality in which this hypothesis holds.

HYPOTHESIS 7.3. *Let $P \in E_v(K) \cap E_\infty(K)$ and $N \geqslant 1$. For fixed $w \mid v$ and $\overline{\infty} \mid \infty$, there exists $\gamma \in \text{Gal}(k^{\text{sep}}/k)$ so that for all embeddings $\tau: K \hookrightarrow k^{\text{sep}}$, we have $\gamma Q_w(\tau P) = Q_{\overline{\infty}}(\tau P)$.*

THEOREM 7.4. *Let E/k be an elliptic curve with ordinary reduction at v and ∞. Let K/k be a global function field. If v (resp. ∞) is ramified in K, we will further assume that E has good reduction at v (resp. ∞). Let $P \in E_v(K) \cap E_\infty(K)$. Suppose that for any N such that $p^N \nmid 2[K:k]\hat{h}_{\text{NT}}(P)$, the point P satisfies Hypothesis 7.3. Then $\widehat{H}_v(P) = \langle P, P \rangle_v \neq 1$.*

We begin with a series of lemmas needed for the proof of Theorem 7.4. Our eventual method will be to compare the values of $\widehat{H}_v$ and $\widehat{H}_\infty$ and to use the known nontriviality of $\widehat{H}_\infty$ to prove that $\widehat{H}_v$ is also nontrivial. This first lemma exhibits one of the peculiarities of characteristic p, especially when compared to number fields. Its proof is fairly standard (see §8.2 of [5]).

LEMMA 7.5. *For any place v of k, let L/k be an algebraic extension such that $L \subset k_v$. Then for every integer $N \geqslant 1$ the map*

$$\frac{L^\times}{(L^\times)^{p^N}} \to \frac{k_v^\times}{(k_v^\times)^{p^N}}$$

is an injection.

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

We take $\omega = dx/(2y + a_1x + a_3)$, α the Hasse invariant of E, and $z = -x/y$ a fixed formal parameter for $\widehat{E}$.

LEMMA 7.6. *Let R be the ring $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6][1/\alpha] \subset k$. Then for all places $w \mid v$ and $w \mid \infty$ of K, the following statements hold.*

(a) *The formal group law for $\widehat{E}/\mathcal{O}_w$ with parameter z is defined over R.*
(b) *For every $m \in \mathbb{Z}$, the division polynomial f_m is an element of $R[x, y]$.*
(c) *The sigma function $\sigma(z) = \sigma_{E/K_w,\omega}(z)$ is given by the formula in (4.2) and, moreover, $\sigma(z) \in R[\![z]\!]$.*

Proof. Recalling the ramification hypotheses on v and ∞ set earlier in the section, the equation for E will be minimal at all places of K extending them, explaining (a) and (b). Part (c) is then a restatement of (4.2). □

LEMMA 7.7. *For every $P \in \widehat{E}(\mathcal{O}_w)$ and integer $N \geqslant 1$,*

$$\sigma_{E/K_w,\omega}(P) \equiv f_{p^N}([p^N]^{-1}(z(P))) \mod (K_w^\times)^{p^N}.$$

Proof. Using (4.2), we find

$$\sigma_{E/K_w,\omega}(P) \equiv \prod_{n=1}^{N} f_p([p^n]^{-1}(z(P)))^{p^{2n-2}} \mod (K_w^\times)^{p^N},$$

and then the result follows by induction on (3.2). □

For an alternate interpretation of $f_{p^N}([p^N]^{-1}(z(P)))$, we consider that, as a function of z, $f_{p^N}(z) = g_{p^N}(z^{p^N})$ is a Laurent series in z^{p^N}. In fact, $g_{p^N} \in k(E^{(p^N)})$, and thus for Q_w as in (7.2),

$$f_{p^N}([p^N]^{-1}(z(P))) = g_{p^N}(V_N^{-1}(z(P))) = g_{p^N}(Q_w). \tag{7.8}$$

Proof of Theorem 7.4. Taking $R = \mathbb{F}_q[a_1, a_2, a_3, a_4, a_6][1/\alpha]$, we note that $R \subset \mathcal{O}_w$ for all $w \mid v$ and $w \mid \infty$. By (7.6) we see that

$$\sigma_{E/K_w,\omega}(z) = \sigma(z),$$

where $\sigma(z)$ is given by the product in (4.2).

By the construction of $\widehat{H}_\infty$ we know that $\widehat{H}_\infty(P)^{[K:k]} \in k_\infty^\times$. The fact that p^N does not divide $2[K : k]\hat{h}_{\mathrm{NT}}(P)$ combined with (6.1) then implies that

$$\widehat{H}_\infty(P)^{[K:k]} \not\equiv 1 \mod (k_\infty^\times)^{p^N}. \tag{7.9}$$

Letting $\langle\ \rangle_v$ and $\langle\ \rangle_\infty$ denote the positive parts with respect to v and ∞, we then have

$$\widehat{H}_\infty(P)^{[K:k]} = H^0(P) \prod_{w|\infty} \left\langle \mathbf{N}_{k_\infty}^{K_w} \sigma(z(P))^{-2} \right\rangle_\infty \in k_\infty^\times,$$

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

where $H^0(P)$ is the product of all the local factors at the finite places. Furthermore, from the construction of $\widehat{H}_v$ we have that

$$\widehat{H}_v(P)^{[K:k]} = \langle H^0(P) \rangle_v \prod_{w|v} \left\langle \mathbf{N}_{k_v}^{K_w} \sigma(z(P))^{-2} \right\rangle_v \in k_v^\times,$$

where $H^0(P)$ is the *same* in both equations. As we will only be interested in these quantities up to p^Nth powers, it is important to note that, for all $x \in k_v^\times$, $x \equiv \langle x \rangle_v$ modulo $(k_v^\times)^{p^N}$, and likewise for $k_\infty^\times$.

Now let $M \subset \mathrm{Gal}(k^{\mathrm{sep}}/k)$ be a set of representatives of the embeddings of $K \hookrightarrow k^{\mathrm{sep}}$. Up to $(k_v^\times)^{p^N}$, we know from (7.7) that

$$\prod_{w|v} \mathbf{N}_{k_v}^{K_w} \sigma(z(P)) \equiv \prod_{w|v} \mathbf{N}_{k_v}^{K_w} f_{p^N}([p^N]^{-1}(z(P))) \mod (k_v^\times)^{p^N}$$

$$\equiv \prod_{\tau \in M} g_{p^N}(Q_w(\tau P)) \mod (k_v^\times)^{p^N},$$

where for some fixed place $w \mid v$ the point $Q_w(\tau P) \in V_N^{-1}(\tau P)$ is defined in (7.2) and (7.8). Likewise, we can show

$$\prod_{w|\infty} \mathbf{N}_{k_\infty}^{K_w} \sigma(z(P)) \equiv \prod_{\tau \in M} g_{p^N}(Q_{\overline{\infty}}(\tau P)) \mod (k_\infty^\times)^{p^N},$$

for some fixed place $\overline{\infty} \mid \infty$ and corresponding $Q_{\overline{\infty}}(\tau P) \in V_N^{-1}(\tau P)$. By (7.9) we then have

$$\widehat{H}_\infty(P)^{[K:k]} \equiv H^0(P) \prod_{\tau \in M} g_{p^N}(Q_{\overline{\infty}}(\tau P))^{-2} \not\equiv 1 \mod (k_\infty^\times)^{p^N}.$$

Likewise, we have

$$\widehat{H}_v(P)^{[K:k]} \equiv H^0(P) \prod_{\tau \in M} g_{p^N}(Q_w(\tau P))^{-2} \mod (k_v^\times)^{p^N}.$$

For both of these two congruences, the right-hand sides are actually elements of k^{sep}. Now by Hypothesis 7.3 the points $Q_w(\tau P)$ and $Q_{\overline{\infty}}(\tau P)$ are simultaneously $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-conjugates, and since $\widehat{H}_\infty(P)^{[K:k]}$ is not a p^Nth power, we conclude that $\widehat{H}_v(P)^{[K:k]}$ is also not a p^Nth power by (7.5). In particular,

$$\widehat{H}_v(P)^{[K:k]} \neq 1,$$

and the theorem follows. □

8. Conditions for Nondegeneracy

The main question of this section is the generality in which Hypothesis 7.3 holds for points in $E_v(K) \cap E_\infty(K)$. As in the previous section, we restrict ourselves to elliptic curves E defined over the rational function field k with ordinary reduction at

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

both v and ∞. We will assume that K/k is Galois. We let $\mathcal{T}_p(E) = \varprojlim \ker V_n$ be the p-adic Tate module. Since E is ordinary, we have $\mathcal{T}_p(E) \cong \mathbb{Z}_p$ as groups. Our main result and an immediate corollary are as follows.

THEOREM 8.1. *Let E/k be an elliptic curve with ordinary reduction at v and ∞. Let K/k be a finite Galois extension. If K is ramified at v (resp. ∞), then we further assume that E has good reduction at v (resp. ∞). Finally, we assume that $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\mathcal{T}_p(E))$ is surjective and that for all places w extending v and ∞ the reduction is good or nonsplit and the $\mathbb{F}_w$-rational p-torsion on the reduction at w is trivial. Then*

(a) $\widehat{H}_v(P) \neq 1$ *for all nontorsion* $P \in E(K)$.
(b) *For all* $P, Q \in E(K)$, *if* $\langle P, Q\rangle_{\mathrm{NT}} \neq 0$, *then* $\langle P, Q\rangle_v \neq 1$.

COROLLARY 8.2. *Under the conditions of Theorem 8.1, the canonical height pairing* $\langle\ ,\ \rangle_v : E(K) \times E(K) \to \mathbb{C}_v^{\times}$ *is nondegenerate.*

The hypotheses in the above theorems are fairly weak, and thus the results hold in some generality. For example, the surjection of the Galois representation is akin to the classical result that an integer is a primitive root modulo p^n, $n \geqslant 2$, if and only if it is a primitive root modulo p^2. Similarly, it is easy to show that $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\mathcal{T}_p(E))$ is surjective if and only if it surjects onto $\mathrm{Aut}(\ker V_2)$.

Let $M \subset E(K)$ be a free Abelian group and consider the tower of field extensions $K \subset K_N \subset L_N$, where $K_N = K(\ker V_N)$ and $L_N = K_N(V_N^{-1}(M))$. If $M = \sum_{i=1}^{r} \mathbb{Z}P_i$ has rank r, there is a natural map

$$\mathrm{Gal}(L_N/K_N) \to (\ker V_N)^r, \tag{8.3}$$

via the Kummer pairing. That is, $\tau \mapsto (\tau Q_i - Q_i)$, where $Q_i \in V_N^{-1}(P_i)$.

The following proposition is a Verschiebung analogue of Bashmakov's Theorem [1, 2], and it uses a Verschiebung descent to show that under certain conditions the image of (8.3) is as large as possible. Since the Verschiebung is separable, such descents behave much like prime-to-p descents, as opposed to the more delicate full p-descent in characteristic p (see [4, 17, 18]). Moreover, the proof is virtually identical to the one found in §V.5 of [7], or see [12] for further details.

PROPOSITION 8.4. *Suppose* $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\mathcal{T}_p(E))$ *is surjective, and let* $M \subset E(K)$ *be a torsion free subgroup of rank* s.

(a) *Let* $M = \mathbb{Z}P$. *If* $P \notin V(E^{(p)}(K))$, *then* $\mathrm{Gal}(L_N/K_N) \cong \ker V_N$.

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

(b) *If* $M \cap V(E^{(p)}(K)) = pM$, *then* $\mathrm{Gal}(L_N/K_N) \cong (\ker V_N)^s$.
(c) *In general, the Kummer pairing induces an isomorphism*

$$\mathrm{Gal}(L_N/K_N) \cong \mathrm{Hom}\left(\frac{M}{M \cap V_N(E^{(p^N)}(K))}, \ker V_N\right).$$

Proof of Theorem 8.1. It suffices to prove the theorem for points P, Q in $E_v(K) \cap E_\infty(K)$. For (a), choosing an N so that

$$p^N \nmid 2\,[K : k]\hat{h}_{\mathrm{NT}}(P),$$

we need to show that P satisfies Hypothesis 7.3. Fixing places $w \mid v$ and $\overline{\infty} \mid \infty$, we need to show that for all embeddings $\tau: K \hookrightarrow k^{\mathrm{sep}}$, the points $Q_w(\tau P)$ and $Q_{\overline{\infty}}(\tau P)$ are simultaneously $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-conjugate.

Let $M = \sum \mathbb{Z}\tau P$, which is torsion-free by the hypotheses on P. By the elementary divisors theorem there is a $\mathbb{Z}$-basis $\{R_i\}$ for M so that

$$\frac{M}{M \cap V_N(E^{(p^N)}(K))} \cong \bigoplus \frac{\mathbb{Z}R_i}{p^{N-k_i}\mathbb{Z}R_i} \quad \text{for } 0 \leqslant k_i \leqslant N.$$

Note that as $p^{N-k_i}R_i \in M \cap V_N(E^{(p^N)}(K))$, our hypothesis that the p^k-torsion $E^{(p^k)}(K)[p^k] = \{O\}$ for all k implies that $R_i \in V_{k_i}(E^{(p^{k_i})}(K))$. Thus via the Kummer pairing with chosen basis $M = \sum \mathbb{Z}R_i$, (8.4c) becomes

$$\mathrm{Gal}(L_N/K_N) \cong \prod \ker V_{N,k_i}, \tag{8.5}$$

where $V_{N,k}$ is the kernel of the Verschiebung $E^{(p^N)} \to E^{(p^k)}$.

By expressing each τP as a linear combination of the R_i, we need to show that there is a $\gamma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ so that

$$\gamma Q_w(R_i) = Q_{\overline{\infty}}(R_i), \quad \text{for all } i. \tag{8.6}$$

First, if $M \cap V(E^{(p)}(K)) = pM$, we apply (8.4b). Then there is an element $\gamma \in \mathrm{Gal}(k^{\mathrm{sep}}/K_N)$ accommodating Hypothesis 7.3, which we lift back to $\mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Second, if $M \cap V_N(E^{(p^N)}(K)) = M$, then for each i we set $Q(R_i)$ to be the unique element of $E^{(p^N)}(K) \cap V_N^{-1}(R_i)$. Indeed, because the p^N-torsion $E^{(p^N)}(K)[p^N] = \{O\}$ by assumption, these two sets meet at only one point. Using the assumptions on the p-torsion on the reductions, we have that $Q(R_i) = Q_w(R_i) = Q_{\overline{\infty}}(R_i)$ for each i.

Finally, in the general case we proceed by combining the above two arguments. For each i, k_i is a largest integer k for which $R_i \in V_k(E^{(p^k)}(K))$. As in the preceding paragraph we have $V_{N,k_i}(Q_w(R_i)) = V_{N,k_i}(Q_{\overline{\infty}}(R_i))$. Thus from (8.5) we find that there is then an automorphism $\gamma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ which satisfies (8.6).

For (b), the proof is much the same as in part (a). By taking N so that $p^N \nmid 2\,[K : k]\langle P, Q\rangle_{\mathrm{NT}}$, an argument similar to the proof of (7.4) shows that we need to have P and Q satisfy Hypothesis 7.3 simultaneously. That is, we require that

there exist $\gamma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ so that

$$\gamma Q_w(\tau P) = Q_{\overline{\infty}}(\tau P) \quad \text{and} \quad \gamma Q_w(\tau Q) = Q_{\overline{\infty}}(\tau Q)$$

for all $\tau: K \hookrightarrow k^{\mathrm{sep}}$. This is achieved by applying the arguments of part (a) to $M = \sum \mathbb{Z}\tau P + \sum \mathbb{Z}\tau Q$. □

Remark 8.7. It should be noted that in (7.4) and (8.1) we have actually proven more than nontriviality. We have shown, under the hypotheses of these theorems, that for $P, Q \in E_v(K) \cap E_\infty(K)$, if $p^N \nmid 2[K:k]\langle P, Q\rangle_{\mathrm{NT}}$, then

$$\langle P, Q\rangle_v^{[K:k]} \not\equiv 1 \mod (k_v^\times)^{p^N}.$$

As pointed out by the referees, the nondegeneracy statement in (8.2) is not strong enough for most conceivable applications. Certainly, what would be better is a statement about the nontriviality of a determinant for the pairing, a difficult question to formulate since the values are taken in the multiplicative group of $\mathbb{C}_v$. However, we prove the following corollary, which shows that, under the hypotheses of (8.1), the pairing $\langle\ ,\ \rangle_v$ is nondegenerate on $E(K) \otimes \mathbb{Z}_p$. This can be used to show the nonexistence of universal norms coming from a certain pro-p-extension of K (see [11, 12]).

COROLLARY 8.8. *Under the conditions of Theorem 8.1, the pairing*

$$\langle\ ,\ \rangle_v: (E(K) \otimes \mathbb{Z}_p) \times (E(K) \otimes \mathbb{Z}_p) \to \mathbb{C}_v^\times$$

is nondegenerate.

Proof. Because the determinant of the Néron–Tate height is non-zero, we know $\langle\ ,\ \rangle_{\mathrm{NT}}$ is nondegenerate on $E(K) \otimes \mathbb{Z}_p$. Thus we suppose $\langle P, Q\rangle_{\mathrm{NT}} \neq 0$ for some $P, Q \in E(K) \otimes \mathbb{Z}_p$. By taking suitable multiples of P and Q we can assume that both are in $(E_v(K) \cap E_\infty(K)) \otimes \mathbb{Z}_p$, and then $p^N \nmid 2[K:k]\langle P, Q\rangle_{\mathrm{NT}}$ for all N large enough. We write

$$P = P_1 + p^N P_2 \quad \text{and} \quad Q = Q_1 + p^N Q_2,$$

where $P_1, Q_1 \in E_v(K) \cap E_\infty(K)$. Then $p^N \nmid 2[K:k]\langle P_1, Q_1\rangle_{\mathrm{NT}}$, and by (8.7), we have that $\langle P_1, Q_1\rangle_v^{[K:k]}$ is not a p^Nth power in $k_v^\times$. Moreover,

$$\langle P, Q\rangle_v = \langle P_1, Q_1\rangle_v \langle P_2, Q_1\rangle_v^{p^N} \langle P_1, Q_2\rangle_v^{p^N} \langle P_2, Q_2\rangle_v^{p^{2N}},$$

and we are done. □

9. An Example

The Mazur–Tate sigma function is effectively computable using (4.2). It is thus possible to compute values of $\widehat{H}_v$ for a given elliptic curve and rational point. For example, suppose E/k is defined over the rational function field and has ordinary

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

reduction at a finite place v. Then on a Weierstrass equation minimal at all finite places, the height of a point $P \in E_v(k)$ is given by

$$\widehat{H}_v(P) = \left\langle \frac{\mathrm{den}(x(P))}{\sigma_{E/k_v,\omega}(P)^2} \right\rangle_v,$$

where $\mathrm{den}(x(P))$ is the denominator of the x-coordinate of P. Thus the v-adic height of P can be obtained by computing values of $\sigma_{E/k_v,\omega}$.

Consider the elliptic curve $E/\mathbb{F}_3(t)$ given by the equation

$$y^2 = x^3 + (t^2-1)x^2 + (t-1)^2(t^2-t-1)^2,$$

which has discriminant $\Delta = (t+1)^3(t-1)^5(t^2-t-1)^2$ and Hasse invariant $\alpha = t^2-1$. In particular, E has ordinary reduction at t. By inspection E has two (linearly independent) k-rational points

$$P = (0, (t-1)(t^2-t-1)), \quad Q = (t^2-t, t^2-1),$$

neither of which is an element of $E_t(k)$. However, calculations will show that $30P$, $30Q \in E_t(k)$. For $z = -x/y$ and $\omega = dx/2y$, the first few terms of $\sigma_{E,\omega}(z)$ are

$$\sigma_{E,\omega}(z) = z - (t^2-1)z^3 + \frac{(t-1)^2(t^2-t-1)^2}{t^2-1}\, z^5 -$$

$$- \frac{t^{11}+t^9+t^5-t^2-1}{(t+1)^6}\, z^7 + \mathrm{O}(z^9)$$

in $\mathbb{F}_3(t)(\!(z)\!)$. Accordingly,

$$\widehat{H}_t(30P) = 1 - t^3 - t^9 + t^{12} + t^{27} - t^{30} - t^{45} + \mathrm{O}(t^{48})$$

and

$$\widehat{H}_t(30Q) = 1 - t^3 + t^{18} - t^{21} + t^{27} + \mathrm{O}(t^{30}).$$

The curve E also has ordinary reduction at ∞, and we can calculate $\widehat{H}_\infty$ similarly. We find that $6P$, $6Q \in E_\infty(k)$, and (with t^{-1} the chosen uniformizer at ∞)

$$\widehat{H}_\infty(6P) = t^{12} - t^{11} + t^{10} + t^8 + t^7 + t^6 + t^5 + \mathrm{O}(t^4)$$

and

$$\widehat{H}_\infty(6Q) = t^{30} - t^{27} - t^{21} + t^{18} - t^3 + 1 + \mathrm{O}(t^{-3}).$$

In terms of Hypothesis 7.3, it is worth noting that $30Q$ satisfies the hypothesis, whereas $30P$ does not, although in both cases the t-adic height is nontrivial.

https://doi.org/10.1023/A:1002054316957 Published online by Cambridge University Press

Acknowledgements

This paper includes some of the results of the author's Brown University PhD thesis, and the author would especially like to thank his advisor, Joseph Silverman, for all of his encouragement and guidance. The author further thanks Antonios Broumas, Michael Rosen, Jeremy Teitelbaum and Siman Wong for many helpful discussions on the contents of this paper. Finally, the author thanks the referees for making many useful comments and suggestions.

References

1. Bashmakov, M.: Un théorème de finitude sur la cohomologie des courbes elliptiques, *C.R. Acad. Sci. Paris Sér. A-B* **270** (1970), A999–A1001.
2. Bashmakov, M.: The cohomology of Abelian varieties over a number field, *Russian Math. Surveys* **27** (1972), 25–70.
3. Bernardi, D.: Hauteurs p-adiques sur les courbes elliptiques, In: M.-J. Bertin (ed.), *Séminaire de Théorie des Nombres, Paris 1979–1980,* Birkhäuser, Boston, 1981, pp. 1–14.
4. Broumas, A.: Effective p-descent, *Compositio Math.* **107** (1997), 125–141.
5. Goss, D.: *Basic Structures of Function Field Arithmetic,* Springer-Verlag, Berlin, 1996.
6. Katz, N. M. and Mazur, B.: *Arithmetic Moduli of Elliptic Curves,* Princeton University Press, Princeton, 1985.
7. Lang, S.: *Elliptic curves*: *Diophantine Analysis,* Springer-Verlag, Berlin, 1978.
8. Mazur, B. and Tate, J.: Canonical height pairings via biextensions, In: M. Artin and J. Tate (eds), *Arithmetic and Geometry*: Papers Dedicated to I. R. Shafarevich on the Occasion of His Sixtieth Birthday, vol. I, Birkhäuser, Boston, 1983, pp. 195–237.
9. Mazur, B. and Tate, J.: The p-adic sigma function, *Duke Math. J.* **62** (1991), 663–688.
10. Mazur, B., Tate, J. and Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84** (1986), 1–48.
11. Papanikolas, M. A.: Universal norms on Abelian varieties over global function fields (in preparation).
12. Papanikolas, M. A.: Canonical heights in characteristic p, Ph.D. thesis, Brown University, Providence, Rhode Island, 1998.
13. Perrin-Riou, B.: Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe, *Invent. Math.* **70** (1982/83), 369–398.
14. Schneider, P.: p-adic height pairings I, *Invent. Math.* **69** (1982), 401–409.
15. Schneider, P.: p-adic height pairings II, *Invent. Math.* **79** (1985), 329–374.
16. Silverman, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves,* Springer-Verlag, New York, 1994.
17. Ulmer, D. L.: p-descent in characteristic p, *Duke Math. J.* **62** (1991), 237–265.
18. Voloch, J. F.: Explicit p-descent for elliptic curves in characteristic p, *Compositio Math.* **74** (1990), 247–258.
19. Voloch, J. F.: An analogue of the Weierstrass ζ-function in characteristic p, *Acta Arith.* **79**(1) (1997), 1–6.