Néron local height functions for elliptic curves

Corina Bianca Panda
Advisor: Dr. Robin de Jong

ALGANT Master's Thesis - July 2013
Université Paris-Sud 11
Universiteit Leiden

Abstract

The goal of this thesis is to look at properties of the local height functions. We prove their order of growth is given by $\lambda([m]P) = O(\log m)$ as $m \to \infty$, which allows us to improve a result of Everest and Ward concerning estimating values of the global canonical height. Then, we look at identities of the local height function which can be used to give slick alternative proofs of results concerning valuations of division polynomials as presented in a paper of Cheon and Hahn. Lastly, we introduce an axiomatic definition of local height functions through a discussion of Green functions at the origin.

Acknowledgements

I am extremely grateful to my advisor, dr. Robin de Jong for his guidance and support throughout the year. This work would have not been possible without his insight and help. I am also thankful to Prof. Bas Edixhoven and dr. Lenny Taelman for sitting on my exam committee and taking the time to read this thesis.

This year in Leiden has been an extraordinary experience. The entire mathematics department at Leiden University has been extremely supportive and welcoming, for which I am very grateful. But mostly, I would like to thank all the Algant students and friends in the department: you made this year unforgettable. Finally, to my family and my loved ones, thank you for everything!

Table of contents

Chapter 1

Introduction

The global canonical height function plays an important role in the arithmetic of elliptic curves. The height is related to important mathematical statements such as the Birch-Swinnerton-Dyer conjecture, thus one hopes to be able to compute the value of heights of rational points on the elliptic curve. The canonical height is introduced as a limit of ordinary heights of points $P \in E(K)\backslash\{O\}$, where E is an elliptic curve over a number field K. Denoted by $\hat{h} : E(\bar{K}) \to [0, \infty)$, the global height function is a quadratic form on E. Moreover, it can be decomposed into sums of local functions that are "almost quadratic", one for each place of K:

$$\hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P) \quad \text{for all } P \in E(K)\backslash\{O\}.$$

The goal of the current thesis is to look at these Néron local height functions and analyze their properties. We prove that the order of growth of these local height functions is given by $\lambda_v([m]P) = O(\log m)$ as $m \to \infty$. This order of growth allows for an improvement of a result of Everest and Ward [6] related to a computational method for estimating the global canonical height of an algebraic point on an elliptic curve. We then look at certain identities involving the local height functions and use them to reprove the results of Cheon and Hahn [4] involving valuations of evaluations of division polynomials at rational points on an elliptic curve. Lastly, we introduce an axiomatic description of the Néron local height function through introducing currents on the "analytification" of E.

This thesis is structured by starting with introducing the necessary preliminaries and then defining the Néron local height functions by giving explicit formulas for both the archimedean and non-archimedean case. Chapter 4 uses these explicit descriptions of the local height function to prove its order of growth is given by $\lambda_v([m]P) = O(\log m)$ when $m \to \infty$. Moreover, we prove that in the case of split multiplicative reduction, the values $\lambda([m]P)$ takes for $m \in \mathbb{Z}_{>0}$ are closely dependent of the order r of P in $E(K)/E_0(K)$.

In Chapter 5 we focus on obtaining identities for the normalized local height function $\tilde{\lambda}$, in particular we prove $\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(P))$ for $P \in E(K)$ non-torsion, $m \in \mathbb{Z}_{>0}$. These identities can be used to obtain results about valuations of division polynomials on the elliptic curve. In particular, we reprove the results of

Cheon and Hahn in [4] in a slick, direct way that avoids lengthy computations and extensive use of properties of division polynomials. At the end of the chapter we go back to look at the global height function and show how the order of growth of $\lambda([m]P)$ allows us to improve a result of Everest and Ward [6] used in computing values of global heights.

While most of the earlier analysis of the local height functions was made explicit by the use of Weierstrass equations and formulas for computing local heights, the goal of the last chapter is to introduce an axiomatic description of these local heights and give a different proof of the identity $\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(P))$. We start with introducing Green functions for a geometrically connected smooth projective curve X over a local field. Looking at the particular case of elliptic curves, we then define local height functions that can be extended in a natural way to currents related to our elliptic curve. These local height functions actually coincide with the normalized Néron local height functions $\tilde{\lambda}$ defined in the earlier chapters. An alternative proof of the aforementioned identity for $\tilde{\lambda}$ can be given using the new description.

Chapter 2

Preliminaries

Elliptic curves are smooth curves of genus one having a specified base point. The goal of this chapter is to introduce basic definitions and notions about the theory of elliptic curves. The following is meant to be a survey of the main results used in the following chapters, for more details see [11], [10].

2.1 Basic notions

Let E be an elliptic curve defined over a perfect field K. Then E can be written as the locus in $\mathbb{P}^2$ of a cubic equation with the base point at ∞, denoted by O. Thus, E can be given by a Weierstrass equation

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$, $i = \overline{1,6}$. The discriminant of the Weierstrass equation is denoted by Δ. Another quantity of interest is the j-invariant of the elliptic curve, defined as $j = c_4^3/\Delta$ where $c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3)$.

Definition 1. Let E_1, E_2 be two elliptic curves. An isogeny from E_1 to E_2 is a non-constant morphism $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$.

Example. For each $m \in \mathbb{Z}$, $m \neq 0$, the multiplication-by-m map $[m] : E \to E$ is an isogeny. Let $E[m](\bar{K})$ denote the m-torsion points on E. To simplify notation, we will write $E[m]$ from now on. If either $\mathrm{char}K = 0$ or $\mathrm{char}K = p, p \nmid m$ we have $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. In this case, $[m]$ is a separable isogeny. Also, $\deg[m] = m^2$ for all $m \in \mathbb{Z}$.

2.2 Division polynomials

Let E/K be an elliptic curve given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define *division polynomials* $\psi_m \in \mathbb{Z}[a_1, ..., a_6, x, y]$ for $m \in \mathbb{Z}_{>0}$ by the initial values

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2y + a_1x + a_3,\\
&\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
&\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),
\end{aligned}$$

where the b_i's are as defined in [11, p. 42], and the recurrence relations

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && \text{for } m \geq 2,\\
\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^3 && \text{for } m \geq 3,
\end{aligned}$$

We then define ϕ_m, ω_m by

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
4y\omega_m &= \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

Since $\Delta \neq 0$, $\psi_m(x)^2$ and $\phi_m(x)$ are relatively prime polynomials in $K[x]$, where $\mathbb{Z}[a_1, ..., a_6, y]$ is seen as a subring of K. In addition, as polynomials in x, we have

$$\begin{aligned}
\phi_m(x) &= x^{m^2} + \text{(lower order terms)}\\
\psi_m(x)^2 &= m^2x^{m^2-1} + \text{(lower order terms)}.
\end{aligned}$$

Proposition 2. *Let $P \in E(\bar{K}), P \neq O$ be a point on the elliptic curve E/K. Then*

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right).$$

Lemma 3. *Let E/K be an elliptic curve, char $K = 0$. For every $m \in \mathbb{Z}_{>0}$, define*

$$F_m(x) = m^2 \prod_{\substack{P\in E[m],\\ P\neq O}} (x - x(P)) \in K(E).$$

By convention we set $F_1(x) = 1$. Then $F_m = \psi_m^2$.

Proof. We compute

$$\operatorname{div}(F_m) = \sum_{P\in E} \operatorname{ord}_P(F_m)(P) = 2\left(\sum_{P\in E[m]} (P)\right) - 2m^2(O).$$

That is because the map $[x : 1] : E \to \mathbb{P}^1$ has a double pole at O and no other poles [11, p.60] and thus $x - x(P)$ has a double pole at O and zeroes at $P, -P \in E[m]$. The identity follows, keeping in mind that $\deg[m] = m^2$.

On the other hand, $\psi_m \in \mathbb{Z}[a_1, ..., a_6, x, y]$ and ψ_m^2 must have a pole at O which has to be of order $m^2 - 1$ since $\psi_m(x)^2 = m^2x^{m^2-1}$ + (lower order terms). Also, $[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$, so ψ_m has a simple zero at $P \in E[m], P \neq O$.

As a result, $\operatorname{div}(F_m) = \operatorname{div}(\psi_m^2)$ and since both have the same coefficient for the x^{m^2-1} term, they must be equal. $\square$

2.3 Reduction modulo π

Let K be a local field complete with respect to a discrete valuation v and let E/K be an elliptic curve. Let π a uniformizer for the ring of integers of K, which we denote by R. Let $\mathcal{M}$ be the maximal ideal of R and $k = R/\pi R$ the residue field.

We can now talk about the reduction of E modulo π. We first choose a minimal Weierstrass equation for E (that is $v(\Delta)$ is minimal subject to the condition that the coefficients are v-integral; such a minimal Weierstrass equation exists by [11, Proposition 1.3, p. 186]). We can now reduce the coefficients modulo π to obtain a curve over the residue field k, namely

$$\tilde{E}: \quad y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6.$$

The curve $\tilde{E}/k$ is called the *reduction of E modulo π*.

The curve $\tilde{E}$ may be singular, but the set of nonsingular points $\tilde{E}_{ns}(k)$ forms a group. Moreover, $E(K)$ admits the following filtration of abelian groups [11, p. 188]:

$$E_1(K) \subset E_0(K) \subset E(K),$$

where

$$E_0(K) = \{P \in E(K) | \tilde{P} \in \tilde{E}_{ns}(k)\},$$
$$E_1(K) = \{P \in E(K) | \tilde{P} = \tilde{O}\}.$$

Here $\tilde{P}$ is the image of $P \in E(K)$ through the reduction map $E(K) \to \tilde{E}(k)$ that sends $P = [x_0 : y_0 : z_0]$ with $x_0, y_0, z_0 \in R$ and at least one in R^*, to $\tilde{P} = [\tilde{x}_0 : \tilde{y}_0 : \tilde{z}_0]$ [11, p.187].

The following result gives information about the structure of the group $E(K)/E_0(K)$ depending on the type of reduction [11, Theorem 6.1, p.200]:

Theorem 4 (Kodaira, Néron)**.** *Let E/K be an elliptic curve. If E has split multiplicative reduction over K, then $E(K)/E_0(K)$ is a cyclic group of order $v(\Delta) = -v(j)$. In all other cases, the group $E(K)/E_0(K)$ is finite and has order at most 4.*

2.4 Formal groups

Let E/K be an elliptic curve defined by a Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

We make a change of variables $z = -\frac{x}{y}, w = -\frac{1}{y}$, so that z is a local uniformizer at O, that is, it has a zero of order 1 at O. O is now the point $(z, w) = (0, 0)$. Let $f(z, w) = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 zw^2 + a_6 w^3$ so the Weierstrass equation for E becomes $f(z, w) = w$. There exists a unique power series $w(z) = z^3(1 + A_1 z + A_2 z^2 + ...) \in \mathbb{Z}[a_1, ..., a_6][\![z]\!]$ such that $w(z) = f(z, w(z))$ [11, p. 116].

Using the power series $w(z)$, we can derive Laurent series for x and y

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - ...$$
$$y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z - ...$$

such that $(x(z), y(z))$ provides a formal solution to the Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Let K be a local field complete with respect to a discrete valuation with ring of integers R and maximal ideal $\mathcal{M}$. If $a_1, ..., a_6 \in R$ then the series $x(z), y(z)$ will converge for any $z \in \mathcal{M}$ and $(x(z), y(z))$ will be a point in $E(K)$. Thus we get an injective map

$$\mathcal{M} \to E(K), \qquad z \mapsto (x(z), y(z)).$$

Definition 5. Let R be a ring. A (one-parameter commutative) formal group $\mathcal{F}$ over R is a power series $F(X, Y) \in R[\![X, Y]\!]$ with the following properties:

1. $F(X, Y) = X + Y +$ (terms of degree ≥ 2)
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity)
3. $F(X, Y) = F(Y, X)$ (commutativity)
4. There is a unique power series $i(T) \in R[\![T]\!]$ such that $F(T, i(T)) = 0$ (inverse)
5. $F(X, 0) = X$ and $F(Y, 0) = Y$.

We call $F(X, Y)$ the formal group law of $\mathcal{F}$.

Example. The formal additive group $\hat{\mathbb{G}}_a$ is defined by $F(X, Y) = X + Y$.

One can define a formal group $\hat{E}$ associated to an elliptic curve E given by a Weierstrass equation with coefficients in R. Here R is the ring of integers of a local field complete with respect to a discrete valuation. Let $z_1, z_2 \in \mathcal{M}$ and $w_1 = w(z_1)$, $w_2 = w(z_2)$. Denote the corresponding points on $E(K)$ by P_1, P_2 respectively. The group law is given by [11, p.119-120]

$$F(z_1, z_2) = i(z_3(z_1, z_2)) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) + ... \in \mathbb{Z}[a_1, ..., a_6][\![z_1, z_2]\!],$$

where $i(z) = \dfrac{x(z)}{y(z) + a_1 x(z) + a_3} \in \mathbb{Z}[a_1, ..., a_6][\![z]\!]$ and $z_3 \in \mathcal{M}$ corresponds to the inverse of $P_1 + P_2$ on $E(K)$. The power series expansion of z_3 is given by

$$z_3 = z_3(z_1, z_2) = -z_1 - z_2 + \frac{a_1 \lambda + a_3 \lambda^2 - a_2 y - 2a_4 \lambda \nu - 3a_6 \lambda^2 \nu}{1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3} \in \mathbb{Z}[a_1, ..., a_6][\![z_1, z_2]\!],$$

where $\lambda = \lambda(z_1, z_2) = \dfrac{w_2 - w_1}{z_2 - z_1}$, $\nu = \nu(z_1, z_2) = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, ..., a_6][\![z_1, z_2]\!]$.

Definition 6. Let $(\mathcal{F}, F)$ be a formal group. We define a multiplication-by-m homomorphism $[m] : \mathcal{F} \to \mathcal{F}$ for $m \in \mathbb{Z}$ by

$$[0](T) = 0, \quad [m+1](T) = F([m](T), T), \quad [m-1](T) = F([m]T, i(T)).$$

The power series expansion for the multiplication-by-m map is given by $[m](T) = mT + (\text{higher-order terms})$.

One can associate a group to every formal group. For the rest of the section we consider K to be a local field complete with respect to some discrete valuation, R its ring of integers, $\mathcal{M}$ the maximal ideal of R and $\mathcal{F}$ a formal group defined over R with group law $F(X, Y)$.

Definition 7. The group associated to $\mathcal{F}/R$, denoted by $\mathcal{F}(\mathcal{M})$, is the set $\mathcal{M}$ endowed with the group operations

$$\begin{aligned} x \oplus_{\mathcal{F}} y &= F(x, y) && \text{(addition)} \quad \text{for } x, y \in \mathcal{M}, \\ \ominus_{\mathcal{F}} x &= i(x) && \text{(inversion)} \quad \text{for } x \in \mathcal{M}. \end{aligned}$$

For $n \geq 1$ we define $\mathcal{F}(\mathcal{M}^n)$ to be the subgroup of $\mathcal{F}(\mathcal{M})$ consisting of the set $\mathcal{M}^n$ with the above group operations.

Example. Let $\hat{E}$ be the formal group associated to an elliptic curve E/K. Then the group associated to $\hat{E}$ is $\hat{E}(\mathcal{M})$. Similarly, the additive group $\hat{\mathbb{G}}_a$ is just $\mathcal{M}$ with the usual addition law.

The reason for introducing the formal group for an elliptic curve is to be able to use the properties of formal groups in the setting of elliptic curves. The following result shows that $E_1(K)$ is in fact a group associated to $\hat{E}$ [11, Proposition 2.2, p.191]:

Proposition 8. *Let E/K be given by a minimal Weierstrass equation, let $\hat{E}/R$ be the formal group associated to E. Then the map*

$$\hat{E}(\mathcal{M}) \to E_1(K), \qquad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)} \right),$$

is an isomorphism of groups.

To understand $E_1(K)$, it is thus enough to understand $\hat{E}(\mathcal{M})$. Introducing the notion of a formal logarithm allows for a homomorphism of $\hat{E}(\mathcal{M})$ to the additive group [11, Theorem 6.4, p.132].

Let K be a field of characteristic 0 and $\mathcal{F}/R$ be a formal group. The formal logarithm of $\mathcal{F}/R$ is a power series in $K[\![T]\!]$ as defined in [11, p. 127]. What is of interest to us is the following description of the logarithm:

Proposition 9. *Let K be of characteristic 0, and $\mathcal{F}/R$ be a formal group. Then*

$$\log_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{c_n}{n} T^n$$

with $c_n \in R$ and $c_1 = 1$.

Theorem 10. *Let K a field of characteristic 0 that is complete with respect to a normalized discrete valuation v, let R be the valuation ring of K, $\mathcal{M}$ the maximal ideal of R, p a prime with $v(p) > 0$ and $\mathcal{F}/R$ a formal group. Let $r > v(p)/(p-1)$ be an integer. Then the formal logarithm induces an isomorphism*

$$\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}^r) \xrightarrow{\sim} \hat{\mathbb{G}}_a(\mathcal{M}^r).$$

2.5 Elliptic curves over $\mathbb{C}$

A lattice in $\mathbb{C}$ is a discrete subgroup that contains an $\mathbb{R}$-basis. That is $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with $\{\omega_1, \omega_2\}$ a basis for $\mathbb{C}$ over $\mathbb{R}$.

Being over $\mathbb{C}$, we can take a Weierstrass equation of the form

$$E : \quad y^2 = x^3 + Ax + B$$

where the discriminant is given by $\Delta = -16(4A^3 + 27B^2)$. Since E is non-singular, $\Delta \neq 0$ and the following uniformization result [10, Corollary 4.3, p.35] holds:

Theorem 11. *Let $A, B \in \mathbb{C}$ with $4A^3 + 27B^2 \neq 0$. Then there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $g_2(\Lambda) = 60G_4(\Lambda) = -4A$ and $g_3(\Lambda) = 140G_6(\Lambda) = -4B$. The map*

$$\begin{aligned} \mathbb{C}/\Lambda &\to E : y^2 = x^3 + Ax + B \\ z &\mapsto \left(\wp(z,\Lambda), \frac{1}{2}\wp'(z,\Lambda)\right) \end{aligned}$$

is a complex analytic isomorphism.

$G_4(\Lambda), G_6(\Lambda)$ are the Eisenstein series of weights 4 and 6 where $G_{2k}(\Lambda)$, the Eisenstein series of weight $2k$, is defined as $G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda,\\ \omega\neq 0}} \omega^{-2k}$. Also, $\wp$ is the Weierstrass $\wp$-function for Λ defined by the series

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda,\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Thus any elliptic curve over the complex numbers is isomorphic to a complex torus $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.

Definition 12. The Weierstrass σ-function is the holomorphic function on $\mathbb{C}$ defined by

$$\sigma(z) = \sigma(z,\Lambda) = z \prod_{\substack{\omega\in\Lambda,\\ \omega\neq 0}} (1 - \frac{z}{\omega}) e^{z/\omega + \frac{1}{2}(z/\omega)^2}.$$

The σ-function has simple zeroes at $z \in \Lambda$ and no other zeroes. Another function of interest is the quasi-periodic map associated to Λ:

Definition 13. The quasi-periodic map $\eta : \Lambda \to \mathbb{C}$ is defined as the difference

$$\eta(\omega) = \zeta(z+\omega, \Lambda) - \zeta(z, \Lambda)$$

where the Weierstrass ζ-function is defined by the series

$$\zeta(z, \Lambda) = \frac{1}{z} + \sum_{\substack{\omega\in\Lambda,\\ \omega\neq 0}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right).$$

2.6 The Tate curve

In the case of elliptic curves over $\mathbb{C}$, we saw that every elliptic curve has a parametrization $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. The goal is to obtain an analogous parametrization when $\mathbb{C}$ is replaced by a p-adic field, that is, a finite extension of $\mathbb{Q}_p$. For this, we introduce the Tate curve [10, Theorem 3.1, p.423]:

Theorem 14 (Tate)**.** *Let K be a p-adic field with absolute value $|\cdot|$, let $q \in K^*$ satisfy $|q| < 1$, and let*

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}, \quad a_4(q) = -s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

1. *The series $a_4(q)$ and $a_6(q)$ converge in K and thus one can define the Tate curve E_q by the equation*

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

2. *The Tate curve is defined over K and has discriminant $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$ and j-invariant $j(E_q) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$ for some integer coefficients $c(n)$.*

3. *The series*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$
$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q),$$

converge for all $u \in \bar{K}^*, u \notin q^{\mathbb{Z}}$. They define a surjective homomorphism

$$\phi : \bar{K}^* \to E_q(\bar{K})$$
$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & if u \notin q^{\mathbb{Z}}, \\ O & if u \in q^{\mathbb{Z}}. \end{cases}$$

The kernel of the map ϕ is $q^{\mathbb{Z}}$.

4. For any algebraic extension L/K, ϕ induces an isomorphism

$$\phi : L^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(L).$$

The group $E_q(K)$ admits the usual filtration

$$E_{q,1}(K) \subset E_{q,0}(K) \subset E_q(K),$$

with $E_{q,0}(K)$, $E_{q,1}(K)$ defined as before. Consider the parametrization of the Tate curve E_q

$$\phi : K^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(K).$$

The map ϕ induces [10, p. 432] the following isomorphism

$$\phi : K^*/R^*q^{\mathbb{Z}} \longrightarrow E_q(K)/E_{q,0}(K).$$

Chapter 3

Local height functions

Let K be a number field and E/K an elliptic curve. For each point $P \in E(K)\backslash\{O\}$, one can define a height function given by

$$h(P) = \frac{1}{2[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{-v(x(P)), 0\}$$

where M_K is the set of places of K, $v(\cdot) = -\log|\cdot|_v$ and $n_v = [K_v : \mathbb{Q}_v]$ is the local degree for $v \in M_K$.

The canonical Néron-Tate height $\hat{h} : E(\bar{K}) \to \mathbb{R}$ is obtained by taking the limit of the ordinary height functions,

$$\hat{h}(P) = \lim_{m \to \infty} \frac{1}{m^2} h([m]P).$$

The canonical height function is a quadratic form, i.e., $\hat{h}$ is an even function and the pairing $\langle \cdot, \cdot \rangle : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$ given by

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

is bilinear [11, Theorem 9.3, p.248]. It is natural to ask whether $\hat{h}$ can be decomposed into sums of quadratic forms, one for each place v of K. While this cannot be done, there exists a decomposition into local height functions that are almost quadratic, in the sense that they satisfy the quasi-parallelogram law.

More exactly, for each place $v \in M_K$, there exists a natural local height function $\lambda_v : E(K_v)\backslash\{O\} \to \mathbb{R}$ such that

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

for all $P \in E(K)\backslash\{O\}$ [10, Theorem 2.1., p.461]. The goal of the following sections is to introduce these Néron local height functions and write explicit formulas for both the archimedean and non-archimedean cases.

3.1 Local Néron height function

Let K be a field complete with respect to an absolute value $|\cdot|_v$ and let $v(\cdot) = -\log|\cdot|_v$. In the non-archimedean case, v is the corresponding valuation. Given E/K an elliptic curve, we will define the local height functions to be certain continuous functions on $E(K)\backslash\{O\}$ with values in $\mathbb{R}$. Here $E(K)\backslash\{O\}$ inherits the topology from $E(K)$, while $\mathbb{R}$ is given its usual topology. The following formulation is due to Tate.

Definition 15. Let K be a complete field and $v(\cdot) = -\log|\cdot|_v$. Let E/K be an elliptic curve with discriminant Δ given by the following Weierstrass equation:

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

1. There is a unique function

$$\lambda : E(K)\backslash\{O\} \to \mathbb{R}$$

satisfying the following properties:

i) λ is continuous on $E(K)\backslash\{O\}$ and is bounded on the complement of any v-adic neighbourhood of O.

ii) The limit

$$\lim_{P\to O}\{\lambda(P) + \frac{1}{2}v(x(P))\}$$

exists.

iii) For all $P \in E(K)\backslash E[2]$ we have

$$\lambda([2]P) = 4\lambda(P) + v((2y + a_1x + a_3)(P)) - \frac{1}{4}v(\Delta).$$

2. λ is independent of the choice of Weierstrass equation for E/K.

3. Let L/K be a finite extension and let w be the extension of v to L. Then

$$\lambda_w(P) = \lambda_v(P) \quad \text{for all } P \in E(K)\backslash\{O\}.$$

The function defined above is called the *local Néron height function* on E associated to v. For a proof of the existence of such a function see [10, Theorem 1.1, p. 455]. One way to renormalize λ, as seen in [9, Second normalisation, p. 90], is by letting

$$\tilde{\lambda}(P) = \lambda(P) - \frac{1}{12}v(\Delta).$$

This renormalization allows for neat functional equations, as we shall see later.

3.2 Archimedean absolute values

Let K be the completion of a number field with respect to an archimedean absolute value and E/K an elliptic curve. Since K embeds into $\mathbb{C}$, questions about points in $E(K)$ can be answered if we look at points in $E(\mathbb{C})$. Thus, we are going to look at the local height function λ over the complex numbers.

Let $E/\mathbb{C}$ be an elliptic curve with corresponding lattice Λ and analytic parametrization given by

$$\phi: \quad \mathbb{C}/\Lambda \to E(\mathbb{C}), \qquad z \mapsto (\wp(z), \wp'(z))$$

where $\wp$ is the Weierstrass $\wp$-function associated to Λ.

The local height function has an explicit description given by the following [10, Theorem 3.2, p. 466] :

Theorem 16. *Let $E/\mathbb{C}$ be an elliptic curve with period lattice Λ. Then the local Néron height function $\lambda : E(\mathbb{C})\backslash\{O\} \to \mathbb{R}$ is given by*

$$\lambda(z) = -\log\left|e^{-\frac{1}{2}z\eta(z)}\sigma(z)\Delta(\Lambda)^{\frac{1}{12}}\right|,$$

where $\eta : \mathbb{C} \to \mathbb{C}$ is the $\mathbb{R}$-linear extension of the quasi-period map $\eta : \Lambda \to \mathbb{C}$.

3.3 Non-archimedean absolute values

Let K be a p-adic field (finite extension of $\mathbb{Q}_p$) for some prime p and let E/K be an elliptic curve. Let v be the corresponding normalized valuation and π a uniformizer for the ring of integers of K, which we will denote by R. Let $\tilde{E}/k$ be the reduction of E modulo π, where $k = R/\pi R$ is the residue field.

In order to be able to work with specific formulas for the local height function, one has to consider the type of reduction of the elliptic curve. The curve E/K has different types of reduction depending on the structure of $\tilde{E}$. Thus, we say that E has *good reduction* if $\tilde{E}$ is nonsingular (that is, $E(K) = E_0(K)$), *multiplicative reduction* if $\tilde{E}$ has a node and *additive reduction* if $\tilde{E}$ has a cusp. In the case of multiplicative reduction, the reduction is said to be split if the slopes of the tangent lines at the node are in k and *nonsplit* otherwise [11, Definition, p.196].

The Semistable reduction theorem [11, Proposition 5.4, p.197] tells us that there exists some finite extension L/K such that E has either good reduction or split multiplicative reduction over L. As the λ function is invariant under finite extensions of K, it is enough to only consider these two cases from now on.

Case 1. If E has good reduction over K, we have $E(K) = E_0(K)$ so we use the following result [10, Theorem 4.1, p.470]:

Theorem 17. *Let K be a field complete with respect to a non-archimedean absolute value. Let v be the corresponding valuation and E/K an elliptic curve described by the Weierstrass equation*

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients are chosen to be v-integral. Let Δ be the discriminant of this equation. Then, the Néron local height function $\lambda : E(K)\backslash\{O\} \to \mathbb{R}$ is given by the formula

$$\lambda(P) = \frac{1}{2}\max\{v(x(P)^{-1}), 0\} + \frac{1}{12}v(\Delta)$$

for all $P \in E_0(K)\backslash\{O\}$.

Notice that if $P \in E_1(K)$ we have $\lambda(P) = -\frac{1}{2}v(x(P)) + \frac{1}{12}v(\Delta)$, otherwise $\lambda(P) = \frac{1}{12}v(\Delta)$ for $P \in E_0(K)\backslash E_1(K)$.

Case 2. In the case where E/K has split multiplicative reduction, E will have multiplicative reduction over any finite extension L/K [11, Proposition 5.4, p.197]. Thus, E does not have potential good reduction, so the j-invariant cannot be integral [11, Proposition 5.5, p.197]. As a result, $|j(E)| > 1$ and by Tate's uniformization theorem [10, Theorem 5.3, p.441], we know there exists a unique $q \in K^*$ with $|q| < 1$ such that E is isomorphic over K to the Tate curve E_q.

The Néron local height function is now given by the following result [10, Theorem 4.2, p.473]:

Theorem 18. *Let K be a p-adic field with valuation $v = -\log|\cdot|$, let $q \in K^*$ satisfy $|q| < 1$, and let E_q/K be the Tate curve with its parametrization*

$$\phi : K^*/q^{\mathbb{Z}} \tilde{\to} E_q(K).$$

i) The Néron local height function $\lambda \circ \phi : (K^*/q^{\mathbb{Z}})\backslash\{1\} \to \mathbb{R}$ is given by the formula

$$\lambda(\phi(u)) = \frac{1}{2}B_2\left(\frac{v(u)}{v(q)}\right)v(q) + v(1-u) + \sum_{n\geq 1} v((1-q^n u)(1-q^n u^{-1})),$$

where $B_2(T) = T^2 - T + \frac{1}{6}$ is the second Bernoulli polynomial.

ii) If we choose $u \in K^*$ to satisfy $0 \leq v(u) < v(q)$, then

$$\lambda(\phi(u)) = \begin{cases} \frac{1}{2}B_2\left(\frac{v(u)}{v(q)}\right)v(q), & \text{if } 0 < v(u) < v(q) \\ v(1-u) + \frac{1}{12}v(q), & \text{if } v(u) = 0. \end{cases}$$

Chapter 4

Order of growth of the Néron local height functions

Let K be the completion of a number field with respect to some absolute value $|\cdot|_v$, E an elliptic curve over K and $\lambda : E(K)\backslash\{O\} \to \mathbb{R}$ the local height function with respect to v. Let P be a non-torsion point in $E(K)$. In the following sections we want to analyze the order of growth of $\lambda([m]P)$. We prove the order of growth is logarithmic, that is $\lambda([m]P) = O(\log m)$ as $m \to \infty$.

4.1 Order of growth in the archimedean case

We are interested in the order of growth of the λ function, more precisely, we are going to show $\lambda([m]P) = O(\log m)$ as $m \to \infty$ for $P \in E(K)$ non-torsion.

Lemma 19. *Let K be the completion of a number field with respect to an archimedean absolute value, E/K an elliptic curve with the corresponding parametrization given by $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ for some lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Let P be non-torsion in $E(K)$ and $z \in \mathbb{C}$ such that $\phi(z \mod \Lambda) = P$. Then $\lambda([m]P) = O(\log |a_m|)$ as $m \to \infty$, where $a_m \in \mathbb{C}$ is the representative of mz in the fundamental parallelogram for Λ.*

Proof. We are going to use the result of Theorem 16. Let F_Λ be the fundamental parallelogram for the lattice, that is $F_\Lambda = \{z \in \mathbb{C} | z = a\omega_1 + b\omega_2 \text{ with a, b } \in [0,1)\}$. Pick $a_m \in F_\Lambda$ such that $a_m = mz \mod \Lambda$. Keeping in mind that the σ function is holomorphic on the whole of $\mathbb{C}$ with simple zeroes at $z \in \Lambda$ and $\Delta(\Lambda)$ is non-zero [11, Proposition 3.6, p. 170], we then have

$$\lambda([m]P) = \frac{1}{2}\operatorname{Re}(a_m\eta(a_m)) - \log|\sigma(a_m)| - \frac{1}{12}\log|\Delta(\Lambda)|.$$

Since $a_m = a\omega_1 + b\omega_2$ for some $a, b \in [0,1)$,

$$|\operatorname{Re}(a_m\eta(a_m))| \le |a_m||\eta(a_m)| \le (|\omega_1| + |\omega_2|)(|\eta(\omega_1)| + |\eta(\omega_2)|).$$

From the definition and properties of σ [11, Definition, Lemma 3.3, p. 167], there exists U a neighborhood of 0 such that

$$\log|\sigma(z)| = \log|z| + \log|f(z)| \quad \text{for all } z \in U\backslash\{0\},$$

where f is a holomorphic function on U non-vanishing at 0. Thus, f must be bounded on U, so there exists a constant $C_1 > 0$ such that $|f(z)| < C_1$ for all $z \in U$. More than that, for sufficiently small U, we can assume f is non-vanishing on the closure of U. Thus, there exists some $C_2 > 0$ such that $|f(z)| > C_2$ for all $z \in U$. So $\log |f(z)|$ is bounded on U, which implies $\log |\sigma(z)| = O(\log |z|)$ as $z \to 0$.

On the other hand, σ is entire, so it is bounded on F_Λ. Thus, there exists $C_3 > 0$ such that $|\sigma(z)| < C_3$ for all $z \in F_\Lambda$. Now let $F'_\Lambda = F_\Lambda \backslash (U \cup U_{\omega_1} \cup U_{\omega_2} \cup U_{\omega_1+\omega_2})$, where $U_{\omega_1}, U_{\omega_2}, U_{\omega_1+\omega_2}$ are translates of U around the other three vertices of the fundamental parallelogram. Thus, σ is going to be non-vanishing on the closure of F'_Λ, so there exists $C_4 > 0$ such that $|\sigma(z)| > C_4$ for all $z \in F'_\Lambda$. Thus, $\log |\sigma(z)|$ is bounded on F'_Λ.

Since P is non-torsion, all points of the form a_m will be distinct as $m \to \infty$. If there is no subsequence of $(a_m)_m$ that tends to either 0 or the other vertices $\omega_1, \omega_2, \omega_1 + \omega_2$ of the fundamental parallelogram, then $\log |\sigma(a_m)|$ is bounded as $m \to \infty$, so $\log |\sigma(a_m)| = O(1)$. If there exist subsequences $(a_{m'})_{m'}$ of $(a_m)_m$ that tend to 0 as $m' \to \infty$, then $\log |\sigma(a_{m'})| = O(\log |a_{m'}|)$ as $m \to \infty$. Similarly, the same reasoning applies if there exist subsequences that tend to the other three vertices of F_Λ.

As a result, since $\frac{1}{2} \operatorname{Re}(a_m \eta(a_m))$ and $-\frac{1}{12} \log |\Delta(\Lambda)|$ are bounded on F_Λ, the order of growth of λ is given by

$$\lambda([m]P) = O(\log |a_m|) \quad \text{as } m \to \infty$$

which ends the proof of the lemma. □

In order to conclude that $\lambda([m]P) = O(\log m)$, we need the following fact on linear forms in elliptic logarithms [1, Proposition 3.3, p.14]:

Theorem 20. *Let E/K be an elliptic curve defined over a number field $K \subset \mathbb{C}$. Fix an isomorphism $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ for an appropriate lattice Λ generated by ω_1, ω_2. Let $P \in E(K)$ be a non-torsion point and $z \in \mathbb{C}$ such that $\phi(z \mod \Lambda) = P$. Then there is a constant $C = C(P) > 0$ such that for all rational numbers l_1/m, l_2/m with $l_1, l_2, m \in \mathbb{Z}$,*

$$\big|z - \big(\frac{l_1}{m}\omega_1 + \frac{l_2}{m}\omega_2\big)\big| \geq e^{-C \max\{1, \log |m|\}}.$$

In the setting of Lemma 19, let ω_1, ω_2 be generators for Λ. Keeping in mind that $mz = a_m + l_1\omega_1 + l_2\omega_2$ for some $l_1, l_2 \in \mathbb{Z}$, we can apply the above result to get $|a_m| \geq m^{-1-C}$ for $m \in \mathbb{Z}_{>0}$ such that $\log m > 1$. On the other hand $\log |a_m|$ is also bounded from above, so

$$(-1 - C) \log m \leq \log |a_m| < C'$$

for some constant $C' > 0$ and m large enough. As a result, we get $\log |a_m| = O(\log m)$ and thus we can conclude that:

Theorem 21. *Let E/K be an elliptic curve over a number field $K \subset \mathbb{C}$ and P a non-torsion point in $E(K)$. The order of growth of the local height function λ with respect to the corresponding archimedean absolute value is given by*

$$\lambda([m]P) = O(\log m),$$

as $m \to \infty$.

4.2 Order of growth in the non-archimedean case

We are interested in the order of growth of the λ function. More specifically, we want to show that if $P \in E(K)$ non-torsion, where K is a number field and v is the valuation corresponding to a non-archimedean place of K, then the order of growth of the associated local height function λ is given by $\lambda([m]P) = O(\log m)$ as $m \to \infty$.

As we have seen in the previous chapter, it is enough to consider the cases when E has either good reduction or split multiplicative reduction. For the case of good reduction, we need the following lemmas:

Lemma 22. *Let K be a p-adic field with valuation v and E/K an elliptic curve. If $P \in E_1(K)$ non-torsion, then $v(x([m]P)) \leq v(x(P))$ for $m \in \mathbb{Z}_{>0}$, with equality if and only if $v(m) = 0$.*

Proof. Let $\mathcal{M}$ be the maximal ideal of R, the ring of integers of K. Choose a minimal Weierstrass equation for E and let $\hat{E}/R$ be the associated formal group. Recall the power series $w(T) = T^3(1 + ...) \in R[[T]]$. As seen in Proposition 8, we have the following isomorphism of groups

$$\hat{E}(\mathcal{M}) \to E_1(K), \qquad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right).$$

The inverse of this map is given by $P \mapsto -\frac{x(P)}{y(P)}$ and since $v(x(P)) < 0$, it is enough to look at the Weierstrass equation to see that $v(x(P)) = -2v(z(P))$, where $z(P) \in \hat{E}(\mathcal{M})$ corresponds to $P \in E_1(K)$.

The multiplication by m map, $[m] : \hat{E} \to \hat{E}$ induces a homomorphism of groups

$$[m] : \hat{E}(\mathcal{M}) \to \hat{E}(\mathcal{M}),$$

where $[m] \in R[[T]$ is given by $[m](T) = mT +$ (higher order terms). For a general term of $[m](z)$, we have $v(a_n z^n) \geq nv(z)$ for $n \geq 2, z \in \mathcal{M}$. Thus $v([m](z)) \geq v(z)$ and notice that we have equality only when $v(m) = 0$.

On the other hand, it is easy to see from the definition of $[m]$ as a formal group homomorphism [11, p.121], that $[m]z(P) = z([m]P)$ for $P \in E_1(K), m \in \mathbb{Z}_{>0}$, where $[m]P$ is the image of P through the multiplication by m map on $E(K)$. As a result, $v(z([m]P)) = v([m]z(P)) \geq v(z(P))$, so $v(x([m]P)) \leq v(x(P))$ for $P \in E_1(K)$, $m \in \mathbb{Z}_{>0}$, with equality if and only if $v(m) = 0$. □

Lemma 23. *Let K be a p-adic field with normalized discrete valuation v and E/K an elliptic curve. Let P a non-torsion point in $E_1(K)$. Then $v(x([m]P)) = -2v(m) + O(1)$ as $m \to \infty$.*

Proof. As in the proof of Lemma 22, let $\mathcal{M}$ be the maximal ideal of the ring of integers of K, $\hat{E}$ the formal group associated to the elliptic curve and $\hat{\mathbb{G}}_a(\mathcal{M})$ the additive group $\mathcal{M}$ with its usual addition. Let r be the smallest integer such that

$r > v(p)/(p-1)$ and by the result of Theorem 6.4 from [11, p. 132] we know the formal logarithm induces an isomorphism

$$\log_{\hat{E}} : \hat{E}(\mathcal{M}^r) \tilde{\to} \hat{\mathbb{G}}_a(\mathcal{M}^r).$$

Moreover, looking at the power series expansion of the formal logarithm [11, Proposition 5.5, p. 129], one can see that $v(z) = v(\log_{\hat{E}} z)$ for $z \in \mathcal{M}^r$. Also remark that since v is normalized, the condition $z \in \mathcal{M}^r$ is equivalent to $v(z) \geq r$.

Now, let $m = p^k m_0$, with $k, m_0 \in \mathbb{Z}_{>0}$, $(m_0, p) = 1$. By Lemma 22, $v(x([m]P)) = v(x([p^k]P))$ for $P \in E_1(K)$. More than that, since $v(z(P)) > 0$ and v normalized, Lemma 22 also tells us that $v(z([p^r]P)) > r$. Thus $z([p^k]P) \in \mathcal{M}^r$ for all $k \geq r-1, k \in \mathbb{Z}$.

As a result, if $k \geq r-1$ we have

$$v(z([p^k]P)) = v(\log_{\hat{E}} z([p^k]P)) = v(p^{k-r} \log_{\hat{E}} z([p^r]P)) = v(p^{k-r+1}) + v(\log_{\hat{E}} z([p^{r-1}]P)),$$

so $v(z([p^k]P)) = v(p^{k-r+1}) + O(1) = v(m) + O(1)$. Since there are only finitely many values that k can take if $k < r-1$, the asymptotic result holds for all $k \in \mathbb{Z}_{\geq 0}$.

On the other hand, as we have already seen in the proof of Lemma 22, $v(x(P)) = -2v(z(P))$ for $P \in E_1(K)$. So $v(x([m]P)) = -2v(m) + O(1)$, which ends the proof. $\square$

Remark. Notice that in the case when $r = 1$, or equivalently, $v(p) < p-1$, the proof of Lemma 23 gives the following equality for all $P \in E_1(K), m \in \mathbb{Z}_{>0}$:

$$v(x([m]P)) = v(x(P)) - 2v(m).$$

Theorem 24. *Let K be a p-adic field with normalized valuation v and E/K an elliptic curve. The associated Néron local height function has an order of growth given by $\lambda([m]P) = O(\log m)$ as $m \to \infty$, where P non-torsion in $E_0(K)$.*

Proof. If $P \in E_1(K)$ the local height function is given by $\lambda(P) = -\frac{1}{2}v(x(P)) + \frac{1}{12}v(\Delta)$. Applying the result of Lemma 23, we get

$$\lambda([m]P) = v(m) + O(1) \quad \text{for all } m \in \mathbb{Z}_{>0}, P \in E_1(K).$$

So the order of growth of the local height function when $P \in E_1(K)$ is given by $O(v(m))$. But it is easy to see that $v(m) = O(\log m)$.

On the other hand, Theorem 17 tells us that for points in $E_0(K) \backslash E_1(K)$ the local height function is a constant given by $\frac{1}{12}v(\Delta)$. We know $E_0(K)/E_1(K) \cong \tilde{E}_{ns}(k)$ [11, Proposition 2.1, p.188], so let r be the order of P in the finite group $E_0(K)/E_1(K)$. Then, the points $[m]P$ with $m \in \mathbb{Z}_{>0}$, $r \nmid m$ are in $E_0(K)$ and $\lambda([m]P) = \frac{1}{12}v(\Delta)$ in this case. We need to see what happens to $\lambda([m]P)$ when m is a multiple of r, but this case has already been treated since these points are in $E_1(K)$, so by the above $\lambda([m]P) = O(\log m)$ when m is a multiple of r, which ends the proof. $\square$

In order to deal with the case of split multiplicative reduction, we need to work with the formulas found in the case of Tate curves. Keeping in mind the filtration of $E(K)$, there are three different cases to analyze for a non-torsion point P. For $P \in E_0(K)\backslash E_1(K)$ or $P \in E_1(K)$, the result of Theorem 24 holds, so the λ function has an order of growth of $\log m$ in those cases. We are left with the case when $P \in E(K)\backslash E_0(K)$, where the order of growth is again logarithmic. The arguments we are going to use are based on the fact that the group $E(K)/E_0(K)$ is finite, in particular it is cyclic of order $v(\Delta) = -v(j)$ in the case of split multiplicative reduction [11, Theorem 6.1, p.200]. In fact, $\lambda([m]P)$ actually takes values in a finite set when $m \in \mathbb{Z}_{>0}$ is not among multiples of r, where r is the order of P in $E_q(K)/E_{q,0}(K)$.

For the rest of the section we are going to work over K a p-adic field with valuation $v = -\log|\cdot|$, $q \in K^*$ such that $|q| < 1$ and E_q/K the Tate curve with its parametrization $\phi : K^*/q^{\mathbb{Z}} \tilde{\to} E_q(K)$.

Lemma 25. *Let P be a non-torsion point in $E_q(K)\backslash E_{q,0}(K)$ with order r in the finite group $E_q(K)/E_{q,0}(K)$. Then, for any integer $1 \le k < r$ we have*

$$\lambda([k]P) = \lambda([r-k]P).$$

Proof. First, by the result of Theorem 18, the value of λ only depends on the class of u in $K^*/q^{\mathbb{Z}}$. Thus, we can choose $u \in K^*$ satisfying $0 \le v(u) < v(q)$ such that $\phi(u) = P$.

Since P has order r in $E_q(K)/E_{q,0}(K)$, the isomorphism $K^*/R^*q^{\mathbb{Z}} \tilde{\to} E_q(K)/E_{q,0}(K)$ tells us there exists some $u_0 \in R^*$ and $N \in \mathbb{Z}$ such that $u^r = u_0 q^N$. On the other hand, for each k we have

$$v(u^k) = v(q)m_k + r_k \text{ where } m_k, r_k \in \mathbb{Z} \text{ with } 0 \le r_k < v(q).$$

Moreover, $r_k = v\left(\dfrac{u^k}{q^{m_k}}\right)$ and since r is the order of P in $E_q(K)/E_{q,0}(K)$, $r_k > 0$. At the same time

$$v(u^{r-k}) = (N - m_k - 1)v(q) + v(q) - r_k.$$

Knowing the classes of the corresponding elements for $[k]P$ and $[r-k]P$ in $K^*/q^{\mathbb{Z}}$, we can now compare their values of λ. We get

$$\begin{aligned}
\lambda([r-k]P) &= \frac{1}{2}B_2\left(\frac{v(q^{m_k+1}) - v(u^k)}{v(q)}\right)v(q) \\
&= \frac{1}{2}B_2\left(\frac{v(q^{m_k}) - v(u^k)}{v(q)} + 1\right)v(q) \\
&= \frac{1}{2}B_2\left(-\frac{v(q^{m_k}) - v(u^k)}{v(q)}\right)v(q) \\
&= \lambda([k]P).
\end{aligned}$$

□

Proposition 26. *Let P be a non-torsion point in $E_q(K)\backslash E_{q,0}(K)$ with order r in the finite group $E_q(K)/E_{q,0}(K)$. Then, for any integers a and k with $1 \leq k < r$ we have*

$$\lambda([k]P) = \lambda([ar \pm k]P).$$

Proof. Let $u \in K^*$ such that $\phi(u) = P$. We then have $\lambda([k]P) = \lambda(\phi(u^k))$ and we can choose u by periodicity such that $0 \leq v(u^k) < v(q)$. In fact, since the order of P in $E_q(K)/E_{q,0}(K)$ is r, we have $0 < v(u^k) < v(q)$.

On the other hand, by the same argument as in the above lemma, there exists $u_0 \in R^*, N \in \mathbb{Z}$ such that $u^r = u_0 q^N$. So the value of $\lambda([ar+k]P)$ only depends on $u^k u_0^a q^{Na}$. But $v(u^k u_0^a) = v(u^k)$, so $\lambda(\phi(u^{ar+k})) = \lambda(\phi(u^k))$ which implies $\lambda([ar+k]P) = \lambda([k]P)$.

We also have $0 < r-k \leq r-1$, so applying the above result we get $\lambda([r-k]P) = \lambda([ar-k]P)$ for any integer a and by the result of the above lemma we are done. □

Theorem 27. *Let K a p-adic field with valuation v, let $q \in K^*$ with $|q| < 1$ and let E_q/K be the corresponding Tate curve. Let P be a non-torsion point in $E_q(K)\backslash E_{q,0}(K)$. Then $\lambda([m]P) = O(\log m)$ as $m \to \infty$.*

Proof. Let r be the order of P in $E_q(K)/E_{q,0}(K)$. Since the group is cyclic of order $v(\Delta)$, r is bounded. Then, we can write $m = ar + k$ for $a, k \in \mathbb{Z}_{>0}$, $0 \leq k < r$.

If $k > 0$, the above proposition tells us that $\lambda([m]P) = \lambda([k]P)$. If $m = ar$, then the point $[r]P$ belongs to $E_{q,0}(K)$ and we have already seen in the proof of Theorem 24 , $\lambda([ar]P) = O(\log a)$, which ends the proof of the theorem. □

Remark. In fact, carefully following the above proofs one can see that we actually get the order of growth to be given by $\lambda([m]P) = O(-\log|m|_v)$ as $m \to \infty$, where $|\cdot|_v$ is the absolute value with respect to which K is complete.

Chapter 5

Identities of the local height functions and applications

The goal of this chapter is to prove some identities of the Néron local height function. In fact, we are going to look at identities of the normalized $\tilde{\lambda}$ function. The next part of the chapter is dedicated to using these identities in reproving the results obtained by J. Cheon and S. Hahn in their paper on "Explicit valuations of division polynomials of an elliptic curve" [4]. Lastly, we look at the global height and use the order of growth of the local heights to improve a result of Everest and Ward [6] on computing the global canonical height of an algebraic point on an elliptic curve.

5.1 The quasi-parallelogram law and a functional equation for $\tilde{\lambda}$

In the following we prove the quasi-parallelogram law and then use it to get a functional equation for the local Néron height function. Recall the normalized Néron local height function for an elliptic curve E over a complete field K with valuation v, was defined in Section 3.1 by $\tilde{\lambda}(P) = \lambda(P) - \frac{1}{12}v(\Delta)$.

Lemma 28. *Let K be a completion of a number field with respect to some absolute value and E/K an elliptic curve. Then, for all points P, Q on the elliptic curve with P, Q, $P \pm Q \neq O$, the normalized Néron local height satisfies the quasi-parallelogram law*

$$\tilde{\lambda}(P+Q) + \tilde{\lambda}(P-Q) = 2\tilde{\lambda}(P) + 2\tilde{\lambda}(Q) + v(x(P) - x(Q)).$$

Proof. First, if the absolute value is archimedean, the result is well known [10, Corollary 3.3, p.467]. For the non-archimedean case when K is a p-adic field, it is enough to prove the result for E having good or split multiplicative reduction over K.

If E has good reduction, we can use the fact that the local Néron height is given by

$$\tilde{\lambda}(P) = \frac{1}{2}\max\{v(x(P)^{-1}), 0\}.$$

Thus, $\tilde{\lambda}(P) = -\frac{1}{2}v(x(P))$ if $P \in E_1(K)$ and $\tilde{\lambda}(P) = 0$ otherwise. We now have to look at all the possible cases:

1. If both P and Q are in $E_1(K)$, then we need to check that

$$v(x(P+Q)) + v(x(P-Q)) = 2v(x(P)) + 2v(x(Q)) - 2v(x(P) - x(Q)).$$

We are in characteristic 0, so let E have the Weierstrass equation given by

$$y^2 = x^3 + Ax + B, \text{ with } A, B \in R.$$

The addition formula [10, Group Law Algorithm 2.3, p.53] gives us the following

$$\begin{aligned} x(P+Q) &= \left(\frac{y(Q) - y(P)}{x(Q) - x(P)}\right)^2 - x(P) - x(Q) \\ &= \frac{(x(P) + x(Q))(A + x(P)x(Q)) + 2B - 2y(P)y(Q)}{(x(P) - x(Q))^2} \\ x(P-Q) &= \frac{(x(P) + x(Q))(A + x(P)x(Q)) + 2B + 2y(P)y(Q)}{(x(P) - x(Q))^2} \end{aligned}$$

so after a bit of algebra we get

$$x(P+Q)x(P-Q) = \frac{(x(P)x(Q) - A)^2 - 4B(x(P) + x(Q))}{(x(P) - x(Q))^2}.$$

Looking at the valuations and keeping in mind the x-coordinates of both P, Q have negative valuations, we notice that if say $v(x(P)) < v(x(Q))$ then

$$v((x(P)x(Q) - A)^2) = 2v(x(P)) + 2v(x(Q)) < v(x(P)) < v(4B(x(P) + x(Q))).$$

In the case when $v(x(P)) = v(x(Q))$, we get again

$$v((x(P)x(Q) - A)^2) < \frac{v(x(P)) + v(x(Q))}{2} \leq v(4B(x(P) + x(Q))).$$

Thus,

$$v((x(P)x(Q) - A)^2 - 4B(x(P) + x(Q))) = 2v(x(P)) + 2v(x(Q))$$

which ends the proof.

2. If $P \in E_1(K)$, $Q \in E_0(K) \backslash E_1(K)$, then we only need to check that

$$v(x(P)) = v(x(P) - x(Q))$$

which is obvious since we have $v(x(P)) < 0$ and $v(x(Q)) \geq 0$.

3. If both $P, Q \in E_0(K)\backslash E_1(K)$, we need to see that $v(x(P)-x(Q)) = 0$. First of all, it is clear the valuation must be non-negative. If we had $v(x(P)-x(Q)) \geq 1$, P, Q would have to reduce to points with the same x-coordinate while the y-coordinates would have to satisfy the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in R.$$

So we'll have either $\widetilde{P} = \widetilde{Q}$ or $\widetilde{P} = -\widetilde{Q}$ and thus either $P+Q$ or $P-Q$ will be in $E_1(K)$, which contradicts our hyphothesis.

If E has split multiplicative reduction, then there exists a unique $q \in K^*$ with $|q| < 1$ such that E is isomorphic over K to the Tate curve E_q with the known parametrization

$$\phi : K^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(K), \quad \phi(u) = (X(u), Y(u)).$$

Choose u_P, $u_Q \in K^*/q^{\mathbb{Z}}$ to satisfy $0 \leq v(u_P), v(u_Q) < v(q)$ such that they are sent to points P, Q under the map ϕ. Since $P, Q \neq O$, we have $v(u_P), v(u_Q) > 0$. We then have

$$\tilde{\lambda}(P+Q) = \frac{1}{2}B\left(\frac{v(u_Pu_Q)}{v(q)}\right)v(q) + v(1-u_Pu_Q) + \sum_{n\geq 1} v((1-q^n(u_Pu_Q)^{-1})(1-q^nu_Pu_Q)$$

$$\tilde{\lambda}(P-Q) = \frac{1}{2}B\left(\frac{v(u_Pu_Q^{-1})}{v(q)}\right)v(q) + v(1-u_Pu_Q^{-1}) + \sum_{n\geq 1} v((1-q^nu_P^{-1}u_Q)(1-q^nu_Pu_Q^{-1})$$

where $B(T) = B_2(T) - \frac{1}{6}$.

It is easy to check that

$$\frac{1}{2}B\left(\frac{v(u_Pu_Q)}{v(q)}\right)v(q) + \frac{1}{2}B\left(\frac{v(u_Pu_Q^{-1})}{v(q)}\right)v(q) = 2\tilde{\lambda}(P) + 2\tilde{\lambda}(Q) + v(u_Q).$$

To finish the proof, we need to use the p-adic θ-function that is defined by the formula

$$\theta(u) = (1-u)\prod_{n\geq 1}\frac{(1-q^nu)(1-q^nu^{-1})}{(1-q^n)^2}.$$

We also know [10, Proposition 3.2, p.429] that

$$X(u_P) - X(u_Q) = -\frac{u_Q\theta(u_Pu_Q)\theta(u_Pu_Q^{-1})}{\theta(u_P)^2\theta(u_Q)^2}.$$

By applying v to this equation and doing a little algebra we find that

$$v(x(P)-x(Q)) = \tilde{\lambda}(P+Q) + \tilde{\lambda}(P-Q) - 2\tilde{\lambda}(P) - 2\tilde{\lambda}(Q).$$

which is exactly what we need. □

Theorem 29. *Let K be a completion of a number field with respect to some absolute value and let E be an elliptic curve over K. The normalized Néron local height function satisfies*

$$\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(P))$$

for all $P \in E(K)$ non-torsion, $m \in \mathbb{Z}_{>0}$.

Proof. We want to give a proof by induction. The trivial cases $m = 1, 2$ are clear from the definitions of the $\tilde{\lambda}$ function and the division polynomials. For $m > 1$, notice that $[m \pm 1]P \neq O$. To finish the proof, we apply the quasi-parallelogram law to points $[m]P$ and P and use the inductive step to get

$$\begin{aligned}\tilde{\lambda}([m+1]P) &= 2\tilde{\lambda}([m]P) + 2\tilde{\lambda}(P) - \tilde{\lambda}([m-1]P) + v(x([m]P) - x(P)) \\ &= (m+1)^2\tilde{\lambda}(P) + 2v(\psi_m(P)) - v(\psi_{m-1}(P)) + v(x([m]P) - x(P)).\end{aligned}$$

But we know that the x-coordinate of $[m]P$ is given by the following ratio of division polynomials

$$x([m]P) = \frac{\phi_m(P)}{\psi_m(P)^2}$$

where the ϕ_m polynomial can be defined by the recurrence relationship

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}.$$

So $v(x([m]P) - x(P)) = v\left(\frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2}\right)$, which is exactly what we need. □

5.2 Applications of the functional equation for $\tilde{\lambda}$

In [4], J. Cheon and S. Hahn estimate valuations of division polynomials and compute them explicitly at singular primes. The approach to prove the results is rather computational and uses properties of division polynomials. On the other hand, we can use the functional equation $\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(P))$ to give slick proofs of the results in [4].

The setting we work in is the following: let K be a number field, R the ring of integers, v the discrete valuation related to a prime ideal $\mathfrak{p}$ of R with $v(\pi) = 1$ for some uniformizer π. Let E be an elliptic curve over K defined by a general Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in R$ for $i = \overline{1, 6}$.

For the next results, we assume P is a non-torsion point in $E(K)\backslash E_0(K)$ of order r in the finite group $E(K)/E_0(K)$. First, we prove the following proposition showing the value of the normalized height function $\tilde{\lambda}$ at the point P is mostly dependent on the order of P in $E(K)/E_0(K)$.

Proposition 30. *Let E/K be an elliptic curve and $P \in E(K)\backslash E_0(K)$ non-torsion of order r in $E(K)/E_0(K)$. Then the normalized Néron local height function is given by*

$$\tilde{\lambda}(P) = -\frac{\mu_P}{2r^2},$$

where $\mu_P = \min(2v(\psi_r(P)), v(\phi_r(P)))$.

Proof. Notice that

$$-\mu_P = \begin{cases} -2v(\psi_r(P)) & \text{if } [r]P \in E_0(K)\backslash E_1(K) \\ -v(\phi_r(P)) & \text{if } [r]P \in E_1(K). \end{cases}$$

On the other hand, $2r^2\tilde{\lambda}(P) = 2\tilde{\lambda}([r]P) - 2v(\psi_r(P))$. If $[r]P \in E_1(K)$, then $\tilde{\lambda}([r]P) = -\frac{1}{2}v(x([r]P))$, so $2r^2\tilde{\lambda}(P) = -v(\phi_r(P))$. If $[r]P \in E_0(K)\backslash E_1(K)$, then $2r^2\tilde{\lambda}(P) = -2v(\psi_r(P))$, which ends the proof. □

Remark. In fact, the above result works over the completion K_v. Notice that $E(K)$, $E_0(K)$ are just restrictions of $E(K_v), E_0(K_v)$. Also, we saw in the last chapter that for fixed non-torsion $P \in E(K_v)\backslash E_0(K_v)$ of order r in $E(K_v)/E_0(K_v)$, $\lambda([m]P)$ takes values in a finite set for $m \in \mathbb{Z}_{>0}$, $r \nmid m$. In particular, $\lambda([k]P) = \lambda([ar \pm k]P)$ for any integers a and k with $1 \leq k < r$. Notice that since $[k]P$ and $[ar \pm k]P$ have the same order in $E(K_v)/E_0(K_v)$ we get the equality $\mu_{[k]P} = \mu_{[ar\pm k]P}$, which tells us that $\mu_{[m]P}$ also takes values in a finite set for $m \in \mathbb{Z}_{>0}, r \nmid m$.

We can now reprove some of the results in [4].

Lemma 31 (Lemma 2, [4])**.** *For any positive integers m and k with $r \nmid k$, we have*

1. $v(\psi_{k-1}(P)\psi_{k+1}(P)) > 2v(\psi_k(P))$
2. $v(\psi_{mr-1}(P)\psi_{mr+1}(P)) = m^2\mu_P$

where $\mu_P = \min(2v(\psi_r(P)), v(\phi_r(P)))$.

Proof. We use the functional equation $v(\psi_m(P)) = \tilde{\lambda}([m]P) - m^2\tilde{\lambda}(P)$ and the quasi-parallelogram law to get

$$\begin{aligned} v(\psi_{k-1}(P)\psi_{k+1}(P)) &= \tilde{\lambda}([k-1]P) + \tilde{\lambda}([k+1]P) - 2(k^2+1)\tilde{\lambda}(P) \\ &= 2\tilde{\lambda}([k]P) - 2k^2\tilde{\lambda}(P) + v(x([k]P) - x(P)) > 2v(\psi_k(P)) \end{aligned}$$

since $v(x([k]P) - x(P)) > 0$. The last inequality is true because P, $[k]P \in E(K)\backslash E_0(K)$ and since there is only one non-singular point on the reduction mod π, we must have $\widetilde{P} = \widetilde{[k]P}$ so then $x([k]P)$ and $x(P)$ are equal modulo π.

For the second part of the lemma, we use the result of Proposition 26 and Proposition 30 to note that

$$\begin{aligned} v(\psi_{mr-1}(P)\psi_{mr+1}(P)) &= \tilde{\lambda}([mr-1]P) + \tilde{\lambda}([mr+1]P) - 2(m^2r^2+1)\tilde{\lambda}(P) \\ &= -2m^2r^2\tilde{\lambda}(P) = m^2\mu_P. \end{aligned}$$

□

Lemma 32 (Lemma 3, [4])**.** *For any positive integers m and k with $1 \leq k < r$ we have*

$$v(\psi_{mr+k}(P)) + v(\psi_{mr-k}(P)) = m^2\mu_P + 2v(\psi_k(P)).$$

Proof. We have

$$\begin{aligned} v(\psi_{mr+k}(P)) + v(\psi_{mr-k}(P)) &= \tilde{\lambda}([mr+k]P) + \tilde{\lambda}([mr-k]P) - 2(m^2r^2+k^2)\tilde{\lambda}(P) \\ &= 2\tilde{\lambda}([k]P) - 2k^2\tilde{\lambda}(P) - 2m^2r^2\tilde{\lambda}(P) \\ &= m^2\mu_P + 2v(\psi_k(P)). \end{aligned}$$

□

Theorem 33 (Theorem 2, [4]). *Let P be a non-torsion point in $E(K)\backslash E_0(K)$ of order r in the finite group $E(K)/E_0(K)$. For any positive integers m and k with $1 \leq k < r$, we have*

$$\begin{aligned} v(\psi_{2mr+k}(P)) &= 2\mu_P m^2 + (2v(\psi_k(P)/\psi_{r-k}(P)) + \mu_P)m + v(\psi_k(P)) \\ v(\psi_{2mr-k}(P)) &= 2\mu_P m^2 - (2v(\psi_k(P)/\psi_{r-k}(P)) + \mu_P)m + v(\psi_k(P)). \end{aligned}$$

Proof. Notice that

$$\begin{aligned} v(\psi_{2mr+k}(P)) &= \tilde{\lambda}([2mr+k]P) - (2mr+k)^2\tilde{\lambda}(P) \\ &= \tilde{\lambda}([k]P) - 4m^2r^2\tilde{\lambda}(P) - 4mrk\tilde{\lambda}(P) - k^2\tilde{\lambda}(P) \\ &= 2\mu_P m^2 - 4mrk\tilde{\lambda}(P) + v(\psi_k(P)). \end{aligned}$$

But

$$\begin{aligned} 2v(\psi_k(P)/\psi_{r-k}(P)) &= 2(r-k)^2\tilde{\lambda}(P) - 2k^2\tilde{\lambda}(P) \\ &= -\mu_P - 4rk\tilde{\lambda}(P), \end{aligned}$$

which proves the first identity. The second identity follows trivially by the same argument. □

Remark. Notice that the above proof of Theorem 2 in [4] only uses the identities in Theorem 29 and Propositions 26 and 30, while [4] makes use of both Lemma 2 and 3 in order to complete the proof. As a result, using the identities of $\tilde{\lambda}$, one can directly obtain the results of Cheon and Hahn, without referring to properties of division polynomials. On the other hand, the proofs we gave for these identities are rather computational as well; a more geometric proof of the result in Theorem 29 will be presented in the next chapter.

5.3 The canonical Néron-Tate height

As seen in a previous chapter, the canonical global height function is a quadratic form $\hat{h}(P) : E(\bar{K}) \to \mathbb{R}$ that can be decomposed into sums of local heights corresponding to the places of the number field K, $\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P)$ for $P \in E(K)\backslash\{O\}$. Thus, computing the value of the global height can be reduced to computing the values of the local heights. The goal of this section is to discuss improvements to a result of Everest and Ward [6] in estimating the global canonical height of an algebraic point on an elliptic curve.

Let K be a number field and E/K an elliptic curve. First, since $\hat{h}(P) = 0$ if and only if P is a torsion point in $E(\bar{K})$ [11, Theorem 9.3., p.249], we are only interested in looking at local heights for points that are non-torsion. Everest and Ward's method of computing the canonical global height is based on the following result [6, Theorem 3]:

Theorem 34. *Let $P \in E(K)$ be a non-torsion point. Let $v \mid \infty$ or v a place corresponding to a prime of singular reduction, where in the case of singular reduction we assume E is given by a Weierstrass equation in minimal form. There are positive constants A and B, $B < 2$ such that*

$$\frac{1}{m^2}\log|\psi_m(P)|_v = \tilde{\lambda}_v(P) + \begin{cases} O((\log m)^A/m^2) & \text{if } v \mid \infty, \\ O(1/m^B) & \text{otherwise.} \end{cases}$$

for all $m \in \mathbb{Z}_{>0}$.

First, notice that the result of Theorem 29 gives us the following:

Proposition 35. *Let K be the completion of a number field with respect to some absolute value $|\cdot|_v$, E/K an elliptic curve and $\tilde{\lambda}_v$ the normalized Néron local height function. Then*

$$\lim_{m\to\infty}\frac{\log|\psi_m(P)|_v}{m^2} = \tilde{\lambda}_v(P)$$

for all $P \in E(K)$ non-torsion.

By the product formula we know that $\prod_{v\in M_K}|x|_v^{n_v} = 1$ for all $x \in K^*$ [11, Product Formula 5.3, p.225], so we get $\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} n_v\tilde{\lambda}_v(P)$. The idea behind Everest and Ward's method lies in estimating the rate of convergence of $\frac{1}{m^2}\log|\psi_m(P)|_v$ as $m \to \infty$ for the infinite places and the ones at which there is bad reduction.

Since

$$\frac{\log|\psi_m(P)|_v}{m^2} = \tilde{\lambda}_v(P) - \frac{\tilde{\lambda}_v([m]P)}{m^2},$$

the order of growth of $\lambda_v([m]P)$ given in the previous chapter improves the result of Theorem 34 above:

Theorem 36. *Let E/K an elliptic curve over a number field and $P \in E(K)$ non-torsion. Then*

$$\frac{\log|\psi_m(P)|_v}{m^2} = \tilde{\lambda}_v(P) + O(\log m/m^2),$$

as $m \to \infty$.

In particular, the value of A that depends on the point P can be taken to be 1 for all P non-torsion in $E(K)$, while the rate of convergence for the places corresponding to primes of bad reduction is also given independently of the point P. In fact, for the second case we actually proved the rate of convergence is given by $O(-\log|m|_v/m^2)$.

Chapter 6

A geometric interpretation of the local height functions through Green functions

The purpose of this section is to give an alternative geometric proof to the identity $\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(x(P)))$. In particular, we will prove the identity for all $P \in E(K)\backslash E[m](K)$, which is a more general result than the one given in Theorem 29.

6.1 An introduction to Green functions

The goal of this section is to introduce the definition of Green functions at the origin for elliptic curves. We start with a survey of facts and properties that work in general for any geometrically connected smooth projective curve X over a local field $(K, |\cdot|)$ and then we restrict to looking at the case of elliptic curves. The following presentation of the theory closely follows Section 2 on the Potential theory on Berkovich analytic curves in [5].

Let X be a geometrically connected smooth projective curve over a local field $(K, |\cdot|)$. We can associate a locally ringed space $\mathfrak{X} = (|\mathfrak{X}|, \mathcal{O}_{\mathfrak{X}})$ to X such that the topological space $|\mathfrak{X}|$ is compact, metrizable, path connected. Moreover, $X(\bar{K})$ is a dense subset of $|\mathfrak{X}|$ and the restriction of the topology from $|\mathfrak{X}|$ to $X(\bar{K})$ coincides with the topology induced from $|\cdot|$. In the case where K is archimedean, $\mathfrak{X} = X(\bar{K})$ as a complex analytic space, while for K non-archimedean, $\mathfrak{X}$ is the so called associated Berkovich space.

Let $\mathcal{A}^0$ be the sheaf of smooth functions on $\mathfrak{X}$ and $\mathcal{A}^1$ the sheaf of smooth forms on $\mathfrak{X}$. In fact, $\mathcal{A}^0$ is a sheaf of $\mathbb{R}$ - algebras, while $\mathcal{A}^1$ is a sheaf of modules over $\mathcal{A}^0$. There exists a Laplace operator $dd^c : \mathcal{A}^0 \to \mathcal{A}^1$, which is known to be the complex Laplacian operator $dd^c = \partial\bar{\partial}/i\pi$ in the archimedean case.

Let $\mathcal{A}^0(\mathfrak{X})$, $\mathcal{A}^1(\mathfrak{X})$ be the spaces of global sections of $\mathcal{A}^0$ and $\mathcal{A}^1$ and $\mathcal{D}^1(\mathfrak{X}) = \mathcal{A}^0(\mathfrak{X})^*$, $\mathcal{D}^0(\mathfrak{X}) = \mathcal{A}^1(\mathfrak{X})^*$ their $\mathbb{R}$-linear duals as $\mathbb{R}$-vector spaces. So the dd^c induces a map from $\mathcal{D}^0(\mathfrak{X})$ to $\mathcal{D}^1(\mathfrak{X})$ such that the diagram commutes

$$\begin{array}{ccc} \mathcal{D}^0(\mathfrak{X}) & \longrightarrow & \mathcal{D}^1(\mathfrak{X}) \\ \uparrow & & \uparrow \\ \mathcal{A}^0(\mathfrak{X}) & \xrightarrow{dd^c} & \mathcal{A}^1(\mathfrak{X}). \end{array}$$

We call this dual map dd^c as well. The upward arrows are injections given by the $\mathbb{R}$-linear pairing $\mathcal{A}^0(\mathfrak{X}) \times \mathcal{A}^1(\mathfrak{X}) \to \mathbb{R}$ defined by $(\varphi, \omega) \to \int_{\mathfrak{X}} \varphi\omega$, where $\int_{\mathfrak{X}} : \mathcal{A}^1(\mathfrak{X}) \to \mathbb{R}$ is the $\mathbb{R}$ -linear integration map known to exist. Thus, for any fixed $\varphi \in \mathcal{A}^0(\mathfrak{X})$, the pairing gives us an $\mathbb{R}$-linear map from $\mathcal{A}^1(\mathfrak{X})$ to $\mathbb{R}$, so $\mathcal{A}^0(\mathfrak{X})$ can be embedded in $\mathcal{D}^0(\mathfrak{X})$, and the same reasoning works for $\mathcal{A}^1(\mathfrak{X}) \hookrightarrow \mathcal{D}^1(\mathfrak{X})$.

Elements of $\mathcal{D}^\alpha(\mathfrak{X})$ are called (α, α)-currents and $(1,1)$-currents can be viewed as measures on $|\mathfrak{X}|$. The goal is to define the Green function as a $(0,0)$-current in $\mathcal{D}^0(\mathfrak{X})$. For that, we need to extend the integration map $\int_{\mathfrak{X}}$ on $\mathcal{D}^1(\mathfrak{X})$. Consider the unit element u of $\mathcal{A}^0(\mathfrak{X})$. Under the natural map $\mathcal{A}^0(\mathfrak{X}) \to \mathcal{D}^1(\mathfrak{X})^*$, u is sent to $\omega \mapsto \omega(u)$. Thus, we define $\int_{\mathfrak{X}} : \mathcal{D}^1(\mathfrak{X}) \to \mathbb{R}$ to be given by $\int_{\mathfrak{X}} \omega = \omega(u)$. Notice that this integration map on $\mathcal{D}^1(\mathfrak{X})$ extends $\int_{\mathfrak{X}}$ on $\mathcal{A}^1(\mathfrak{X})$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{D}^1(\mathfrak{X}) & \longrightarrow & \mathbb{R}. \\ \uparrow & \nearrow & \\ \mathcal{A}^1(\mathfrak{X}) & & \end{array}$$

Let $P \in X(\bar{K})$. Given the $dd^c : \mathcal{D}^0(\mathfrak{X}) \to \mathcal{D}^1(\mathfrak{X})$, we can now define the Green function at P as a $(0,0)$-current in the following way:

Definition 37. Let $\mu \in \mathcal{A}^1(\mathfrak{X})$ be a normalized smooth measure with $\int_{\mathfrak{X}} \mu = 1$. Then, there exists a unique current $g_{\mu,P} \in \mathcal{D}^0(\mathfrak{X})$ that satisfies

1. $dd^c g_{\mu,P} = \mu - \delta_P$
2. $\int_{\mathfrak{X}} g_{\mu,P}\mu = 0$,

where $\delta_P \in \mathcal{D}^1(\mathfrak{X})$ is the Dirac measure at the point $P \in X(K)$.

We want to be able to evaluate currents $g_{\mu,P}$ at points in $X(\bar{K})$. First, the $\mathbb{R}$-linear pairing $\mathcal{A}^0(\mathfrak{X}) \times \mathcal{A}^1(\mathfrak{X}) \to \mathbb{R}$ extends to a pairing $\mathcal{D}^0(\mathfrak{X}) \times \mathcal{D}^1(\mathfrak{X}) \to \mathbb{R}$ given by $(\varphi, \omega) \to \int_{\mathfrak{X}} \varphi\omega$. Thus, one can define $g_{\mu,P}(Q) = \int_{\mathfrak{X}} g_{\mu,P}\delta_Q$.

Another fact we need is that given a non-zero rational function f on $X \otimes \bar{K}$, $\log|f|$ can be extended in a natural way as a $(0,0)$-current. Lastly, one needs mentioning that we can define a canonical probability measure on $|\mathfrak{X}|$ that we shall denote by $\mu_{\mathfrak{X}} \in \mathcal{A}^1(\mathfrak{X})$.

6.2 The case of elliptic curves

Let K be a number field and consider the completions K_v at all places of K. Let E/K_v be an elliptic curve and denote the associated ringed space by $\mathcal{E}_v$. In the following we give another definition of the local height function on $E(K)\backslash\{O\}$. We see this function can be uniquely extended to an $(0,0)$-current on $\mathcal{E}_v$.

6.2.1 The topology and measure on $E(K)$

First, we consider the non-archimedean case. Let K be a p-adic field with normalized discrete valuation v. Let R be the ring of integers, π a uniformizer and $\mathcal{M} = \pi R$ the maximal ideal. Since the residue field k is finite, we know that K must be locally compact with respect to the p-adic topology [3, Corollary, p.50]. Moreover, let U be a compact neighborhood of O. Then, for c large enough, $\pi^c R \subset U$ and since $\pi^c R$ is closed, it is also compact. As a result, R must be compact as well.

Let E/K be an elliptic curve. The goal is to give $E(K)$ a topology with respect to which it is compact. For that, endow $K \times K \times K$ with the product topology inherited from the p-adic topology on K, and $K^3\backslash(0,0,0)$ with the subspace topology. Then $\mathbb{P}^2(K)$ will have a quotient topology via $K^2\backslash(0,0,0) \to \mathbb{P}^2(K)$. More than that, $\mathbb{P}^2(K)$ is the union of the images of the open sets $R^\times \times R \times R$, $R \times R^\times \times R$ and $R \times R \times R^\times$, which are compact. Thus, $\mathbb{P}^2(K)$ will also be compact for the topology just defined. As a subset of $\mathbb{P}^2(K)$ via the Weierstrass equation, $E(K)$ can be endowed with the subspace topology. Since $\mathbb{P}^2(K)$ is compact, $E(K)$ will also be compact since it is closed, so we proved the following:

Lemma 38. *Let K be a p-adic field and E/K an elliptic curve. Then $E(K)$ has a natural topology induced by the topology on K with respect to which it is compact.*

Notice that the above topology on $E(K)$ is the same as the v-adic topology mentioned in Section 3.1, where the valuation v is p-adic in this case. In this topology, two points are "close" if and only if their coordinates are "close" in the p-adic topology of K. Moreover, one can check summing two points on $E(K)$ and taking inverses are continuous operations, so $E(K)$ is in fact a topological group. Thus, there exists a left Haar measure on $E(K)$ which we denote by μ_E. Since $E(K)$ is compact, we have $0 < \mu_E(E(K)) < \infty$, so we can normalize the measure so that $\mu_E(E(K)) = 1$. Notice that since $E(K)$ is abelian, it is unimodular, so the left Haar measure is also a right Haar measure [7, p.312-321].

For the archimedean case, let K be the completion of a number field with respect to an archimedean absolute value. In this setting, we know $E(\mathbb{C})$ is isomorphic to a torus $\mathbb{C}/\Lambda$ for some lattice Λ. Therefore, $E(K)$ inherits the complex topology on $\mathbb{C}$ with respect to which it is compact. Being a topological group, there exists a Haar measure that can be normalized, just like in the non-archimedean situation.

6.2.2 Restrictions of Green functions at the origin

Taking our smooth projective curve to be an elliptic curve over the completion of a number field K with respect to some place v, denote the associated ringed space by $\mathcal{E}_v$. Let μ_v be the canonical probability measure on the topological space of $\mathcal{E}_v$. We then have a Green function at the origin defined as seen in the previous section:

Definition 39. There exists a unique current $g_{\mu_v,O} \in \mathcal{D}^0(\mathcal{E}_v)$ that satisfies

1. $dd^c g_{\mu_v,O} = \mu_v - \delta_O$
2. $\int_{\mathcal{E}_v} g_{\mu_v,O} = 0,$

where $\delta_O \mathcal{D}^1(\mathcal{E}_v)$ is the Dirac measure at the origin. We call this current the Green function at the origin.

Definition 40. Let $g_{\mu_v,O}$ be the Green function at the origin. Let $\hat{\lambda} : E(K)\backslash\{O\} \to \mathbb{R}$ be the restriction

$$\hat{\lambda} = g_{\mu_v,O}|_{E(K)\backslash\{O\}}.$$

Notice that since the Haar measure is the unique translation invariant measure up to a constant, when we restrict the canonical measure μ_v on $\mathcal{E}_v$ to $E(K)$, we must get the Haar measure on $E(K)$. Thus, being the restriction of $g_{\mu_v,O}$ to $E(K)\backslash\{O\}$, the $\hat{\lambda}$ function is the unique smooth function on $E(K)\backslash\{O\}$ that satisfies

1. $dd^c\hat{\lambda} = \mu_E - \delta_O$
2. $\int_{E(K)} \hat{\lambda}\mu_E,$

where μ_E is the normalized Haar measure on $E(K)$. We will see later that in fact the restriction $\hat{\lambda}$ defined above coincides with the Néron local height function as given in Definition 15.

6.2.3 Identities of the restriction $\hat{\lambda} = g_{\mu_v,O}|_{E(K)\backslash\{O\}}$

The goal of this section is to use the functoriality of Green functions on $\mathcal{E}_v$ to obtain certain identities involving their restrictions to points on $E(K)\backslash\{O\}$.

Proposition 41. *Let $\phi : E_1 \to E_2$ be an isogeny between elliptic curves over the completion K of a number field with respect to one of its places. Let $\hat{\lambda}_{E_1}, \hat{\lambda}_{E_2}$ be the corresponding restrictions of the Green functions of the origin for E_1, E_2. Then $\phi_*\hat{\lambda}_{E_1} = \hat{\lambda}_{E_2}$, that is $\sum_{\phi(Q)=P} \hat{\lambda}_{E_1}(Q) = \hat{\lambda}_{E_2}(P)$ for all $P \in E_2(K)\backslash\{O\}$.*

Proof. First, since μ_{E_1}, μ_{E_2} are the normalized Haar measures on $E_1(K), E_2(K)$, we have $\phi_*\mu_{E_1} = \mu_{E_2}$. That is because $\phi : E_1(K) \to E_2(K)$ is a continuous surjective homomorphism between compact groups, so $\phi_*\mu_{E_1}$ must be a Haar measure on $E_2(K)$ and then we are done because of the unicity of Haar measures and the fact that both $\phi_*\mu_{E_1}$ and μ_{E_2} are normalized [8, Lemma 1.3.1, p.25].

We have $\phi_*\hat{\lambda}_{E_1}$ a smooth function on $E_2(K)\backslash\{O\}$, so because of the way the restriction $\hat{\lambda}$ function is defined above, it is enough to prove $\phi_*\hat{\lambda}_{E_1}$ satisfies

1. $dd^c\phi_*\hat{\lambda}_{E_1} = \mu_{E_2} - \delta_O$
2. $\int_{E_2(K)} \phi_*\hat{\lambda}_{E_1}\mu_{E_2} = 0.$

For the first identity, we have

$$\begin{aligned} dd^c\phi_*\hat{\lambda}_{E_1} &= \phi_* dd^c\hat{\lambda}_{E_1} \\ &= \phi_*(\mu_{E_1} - \delta_O) \\ &= \phi_*\mu_{E_1} - \phi_*\delta_O \\ &= \mu_{E_2} - \delta_{\phi(O)} = \mu_{E_2} - \delta_O. \end{aligned}$$

We are left to check $\int_{E_2(K)} \phi_*\hat{\lambda}_{E_1}\mu_{E_2} = 0$. By the result of Theorem 3.6.1 in [2, p.190], we have

$$\begin{aligned} \int_{E_2(K)} \phi_*\hat{\lambda}_{E_1}\mu_{E_2} &= \int_{E_2(K)} \phi_*\hat{\lambda}_{E_1}(\phi_*\mu_{E_1}) \\ &= \int_{E_1(K)} \phi^*(\phi_*\hat{\lambda}_{E_1})\mu_{E_1}. \end{aligned}$$

But $\phi^*\phi_*\hat{\lambda}_{E_1}(P) = \phi_*\hat{\lambda}_{E_1(K)}(\phi(P)) = \sum_{P-Q\in\ker\phi} \hat{\lambda}_{E_1}(Q)$ for all $P \in E_1(K)$, so

$$\begin{aligned} \int_{E_2(K)} \phi_*\hat{\lambda}_{E_1}\mu_{E_2} &= \int_{E_1(K)} \phi^*\phi_*\hat{\lambda}_{E_1(K)}(P)\mu_{E_1}(P) \\ &= \int_{E_1(K)} \sum_{P-Q\in\ker\phi} \hat{\lambda}_{E_1(K)}(Q)\mu_{E_1}(P) \\ &= \sum_{R\in\ker\phi} \int_{E_1(K)} \hat{\lambda}_{E_1(K)}(P-R)\mu_{E_1}(P) \\ &= \sum_{R\in\ker\phi} \int_{E_1(K)} \hat{\lambda}_{E_1(K)}\mu_{E_1} = 0 \end{aligned}$$

since μ_{E_1} is translation invariant. □

Corollary. *Let E be an elliptic curve over the completion K of a number field and $\hat{\lambda}$ the corresponding restriction of the Green function at the origin. Then*

$$\sum_{[m]Q=O} \hat{\lambda}(P+Q) = \hat{\lambda}([m]P)$$

for all $P \in E(K)\backslash E[m](K)$, $m \in \mathbb{Z}_{>0}$.

Proof. The solution follows trivially from the above Proposition by considering the multiplication-by-m map as an isogeny on E. □

Lemma 42. *Let K be the completion of number field with absolute value $|\cdot|_v$, E/K an elliptic curve and $\hat{\lambda}$ the corresponding restriction of the Green function at the origin. Then*

$$\sum_{\substack{[m]Q=O,\\ Q\neq O}} \hat{\lambda}(Q) = -\log|m|_v.$$

Proof. From the above Corollary, we have that $\sum_{\substack{[m]Q=O,\\ Q\neq O}} \hat{\lambda}(P+Q) = \hat{\lambda}([m]P) - \hat{\lambda}(P)$.

As $\hat{\lambda}$ is continuous on $E(K)\backslash\{O\}$, it is enough to find the limit as $P \to O$ of $\hat{\lambda}([m]P) - \hat{\lambda}(P)$.

It is a fact that $\lim_{P\to O}\{\hat{\lambda}(P) - \frac{1}{2}\log|x(P)|_v\}$ exists. As a result, we have

$$\lim_{P\to O}\{\hat{\lambda}([m]P) - \hat{\lambda}(P) - \frac{1}{2}\log|x([m]P)|_v + \frac{1}{2}\log|x(P)|_v\} = 0.$$

In the non-archimedean case, K is a p-adic field with valuation $v(\cdot) = -\log|\cdot|_v$. Let r be the smallest integer such that $r > v(p)/(p-1)$, $\mathcal{M}$ the maximal ideal of the ring of integers of K, $\hat{E}$ the formal group associated to the elliptic curve and $z(P) \in \hat{E}(\mathcal{M})$ corresponding to some $P \in E_1(K)\backslash E[m](K)$ such that $z(P) \in \mathcal{M}^r$.

By the same reasoning as in the proof of Lemma 23, we get that $v(z([m]P)) = v(m) + v(z(P))$. So

$$v(x([m]P)) = -2v(m) + v(x(P)).$$

Consequently, $-\frac{1}{2}\log|x(P)|_v + \frac{1}{2}\log|x([m]P)|_v = -\log|m|_v$ which ends the proof in this case.

In the case of an archimedean absolute value $|\cdot|$, let $E/\mathbb{C}$ be our elliptic curve with period lattice Λ. Let $z \in \mathbb{C}/\Lambda$ corresponding to P on $E(\mathbb{C})$. Then, the x-coordinate of P is given by the Weierstrass $\wp$-function. Since $\wp$ has a double pole at the lattice points, there exists a neighborhood U around the origin such that

$$\log|\wp(z)| = \log|f(z)| - 2\log|z| \quad \text{for all } z \in U\backslash\{O\},$$

where f is a holomorphic function non-vanishing on U. We can assume both $z, mz \in U$, so for all such z distinct from 0 we have

$$\frac{1}{2}\log|\wp(mz)| - \frac{1}{2}\log|\wp(z)| = \frac{1}{2}\log|f(mz)| - \frac{1}{2}\log|f(z)| - \log|m|.$$

Taking the limit as z goes to 0, we get $\frac{1}{2}\log|\wp(mz)| - \frac{1}{2}\log|\wp(z)| \to -\log|m|$, which ends the proof. □

6.2.4 Local height functions

It was mentioned in an earlier section that the restriction of the Green function at the origin to points on $E(K)\backslash\{O\}$ coincides with the Néron local height function introduced in Chapter 2. In the following, we give a proof of this fact.

Theorem 43. *Let E/K an elliptic curve defined over the completion of a number field with respect to an absolute value $|\cdot|_v$, let $g_{\mu_v,O}$ be Green function at the origin and $\hat{\lambda} : E(K)\backslash\{O\} \to \mathbb{R}$ its restriction to the space $E(K)\backslash\{O\}$. Then the restricted $\hat{\lambda}$ function coincides to the Néron local height function λ as given by Definition 15.*

Proof. We know the normalized local height function $\tilde{\lambda}$ satisfied the quasi-parallelogram law as seen in Section 5.1:

$$\tilde{\lambda}(P+Q) + \tilde{\lambda}(P-Q) = 2\tilde{\lambda}(P) + 2\tilde{\lambda}(Q) + v(x(P) - x(Q))$$

for all $P, Q \in E(K)\backslash\{O\}$ such that $P \pm Q \neq O$. One can give an equivalent definition of the $\tilde{\lambda}$ function in the following way. First, since $x - x(P)$ is a non-zero rational function on $E \otimes \bar{K}$, $\log|x - x(P)|_v$ extends as a $(0,0)$-current on $\mathcal{E}_v$, so by fixing $P \in E(K)\backslash\{O\}$, we can integrate the quasi-parallelogram law against $\mu_v(Q)$. Keeping in mind that the canonical probability measure μ_v on $\mathcal{E}_v$ is translation invariant, we get

$$\tilde{\lambda}(P) = \frac{1}{2}\int_{\mathcal{E}_v} \log|x - x(P)|_v \mu_v \quad \text{for all } P \in E(K)\backslash\{O\}.$$

But $\tilde{\lambda}(P) = \lambda(P) + \frac{1}{12}\log|\Delta|_v$. As a result, the Néron local height function described in Chapter 3 is given by

$$\lambda(P) = \frac{1}{2}\int_{\mathcal{E}_v} \log|x - x(P)|_v \mu_v - \frac{1}{12}\log|\Delta|_v$$

for all $P \in E(K)\backslash\{O\}$.

On the other hand, $\frac{1}{2}\int_{\mathcal{E}_v} \log|x - x(P)|_v \mu_v$, and thus $\tilde{\lambda}$, can be uniquely extended in a natural way as a $(0,0)$-current on $\mathcal{E}_v$, as seen in [5, Theorem 4.3]. Moreover, it satisfies the dd^c equation

$$dd^c\tilde{\lambda} = \mu_v - \delta_O.$$

Since $\lambda = \tilde{\lambda} - \frac{1}{12}\log|\Delta|_v$, λ can also naturally and uniquely extend to a $(0,0)$-current $\hat{g}_{\mu_v,O}$ on $\mathcal{E}_v$. Thus, the current $\hat{g}_{\mu_v,O}$ also satisfies the dd^c equation

$$dd^c\hat{g}_{\mu_v,O} = \mu_v - \delta_O.$$

Notice that $g_{\mu_v,O}$ and $\hat{g}_{\mu_v,O}$ satisfy the same dd^c equation, so we have [5, Theorem 4.3]

$$\hat{g}_{\mu_v,O}(P) = g_{\mu_v,O}(P) + \int_{\mathcal{E}_v} \hat{g}_{\mu_v,O}\mu_v,$$

for all $P \in E(K)\backslash\{O\}$. Restricting this identity to $E(K)\backslash\{O\}$, we get $\lambda(P) = \hat{\lambda}(P) + \int_{\mathcal{E}_v} \hat{g}_{\mu_v,O}\mu_v$. Thus, we are done once we prove $\int_{\mathcal{E}_v} \hat{g}_{\mu_v,O}\mu_v = 0$.

First, by a similar argument as the one given in Proposition 5.1 of [5] we get the following:

$$\tilde{\lambda}(P_i) = \frac{1}{2}\int_{\mathcal{E}_v} \log|x - x(P_i)|_v \mu_v = \frac{1}{4}\log|f'(\alpha_i)|_v,$$

where E is given by $y^2 = f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ with $\alpha_i = x(P_i)$ the x-coordinates of the non-zero 2-torsion points of E over $\bar{K}$. We know $\Delta = 16\prod_{i=1}^3 f'(\alpha_i)$, so then

$$\sum_{i=1}^{3} \lambda(P_i) = \frac{1}{4}\log\left|\Delta/16\right|_v - \frac{1}{4}\log|\Delta|_v = -\log|2|_v.$$

On the other hand, Lemma 42 tells us that $\sum_{i=1}^3 \hat{\lambda}(P_i) = -\log|2|_v$ and thus we have $3\int_{\mathcal{E}_v} \hat{g}_{\mu_v,O}\mu_v = 0$, which forces $\hat{\lambda} = \lambda$ and ends the proof. $\square$

6.3 Alternative proof of the identity $\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(x(P)))$

In the above section, we gave an alternative definition of Néron local height functions as restrictions of Green functions at the origin. The goal of this section is to use the properties of these restrictions to give a more geometric proof of the main result of Theorem 29.

Theorem 44. *Let K be the completion of a number field with respect to an absolute value $|\cdot|_v$, $v(\cdot) = -\log|\cdot|_v$ and let E/K be an elliptic curve over K. The normalized local height function satisfies*

$$\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + v(\psi_m(P)),$$

for all $P \in E(K)\backslash E[m](K)$, $m \in \mathbb{Z}_{>0}$.

Proof. We know the normalized local height function satisfies the quasi-parallelogram law

$$\tilde{\lambda}(P+Q) + \tilde{\lambda}(P-Q) = 2\tilde{\lambda}(P) + 2\tilde{\lambda}(Q) + v(x(P) - x(Q))$$

for $P, Q, P \pm Q \neq O$. Summing over $Q \in \ker[m], Q \neq O$ we get

$$2\sum_{\substack{Q\in\ker[m],\\ Q\neq O}} \tilde{\lambda}(P+Q) = 2(m^2-1)\tilde{\lambda}(P) + 2\sum_{\substack{Q\in\ker[m],\\ Q\neq O}} \tilde{\lambda}(Q) + \sum_{\substack{Q\in\ker[m],\\ Q\neq O}} v(x(P)-x(Q))$$

Notice that since local height functions are invariant under finite extensions of the base field, we can assume K such that all m-torsion points are in $E(K)$. Thus, $\tilde{\lambda}(P+Q)$ makes sense for all $Q \in \ker[m]$.

Using Lemma 42, the Corollary to Proposition 41 and the fact that the restriction $\hat{\lambda}$ coincides with the Néron local height λ we have

$$\lambda([m]P) = m^2\lambda(P) + v(m) + \frac{1}{2}\sum_{\substack{Q\in\ker[m],\\ Q\neq O}} v(x(P)-x(Q)).$$

Notice that the proof is complete since we know $\psi_m(x)^2 = m^2 \prod_{\substack{Q\in E[m],\\ Q\neq O}} (x - x(Q))$.

□

Bibliography

[1] M. Baker, S. Ih, and R. Rumely. A finiteness property of torsion points. *Algebra & Number Theory*, page 217, 2008.

[2] V. I. Bogachev. *Measure theory*, volume 1. Springer, 2007.

[3] J. W. S. Cassels and A. Fröhlich. *Algebraic number theory: proceedings of an instructional conference*. Academic Press, 1967.

[4] J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. *Manuscripta Mathematica*, 97(3):319–328, 1998.

[5] R. de Jong. Local heights on Galois covers of the projective line. *Acta Arithmetica*, 152:51–70, 2012.

[6] G. Everest and T. Ward. The canonical height of an algebraic point on an elliptic curve. *New York Journal of Mathematics*, 6(331):342, 2000.

[7] G. B. Folland. *Real analysis: modern techniques and their applications*, volume 2. Wiley New York, 1984.

[8] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Society, 1999.

[9] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Friedrick Vieweg & Son, 1997.

[10] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, 1994.

[11] J.H. Silverman. *The arithmetic of elliptic curves*. Springer, 2009.