COMPUTING CANONICAL HEIGHTS ON ELLIPTIC CURVES

Matthew Warren

Computing Canonical Heights on Elliptic Curves

Easter Term 2024

Contents

1 Introduction

Given an elliptic curve E over a number field K, the Mordell-Weil theorem states that

$$E(K) \cong T \times \mathbb{Z}^r,$$

for some finite abelian group T, and $r \in \mathbb{N}$ the rank. It is therefore of considerable interest to compute a basis of the group $E(K)/T \cong \mathbb{Z}^r$. If T and r are known, the general strategy ([Cre97, p. 75-78]) to compute generators begins by finding a set of r linearly independent points on $E(K)$. To test linear independence of a set of points $P_1, \ldots, P_s$, one must calculate the determinant $\det(\langle P_i, P_j \rangle)$, where $\langle \cdot, \cdot \rangle$ is the Neron-Tate bilinear form

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

with $\hat{h} : E \to \mathbb{R}$ the *canonical height*. Thus, practical computation of the canonical height is of great importance in finding independent sets of points on $E(K)$, which we shall explore is Part II of this essay. Having found independent points $Q_1, \ldots, Q_r \in E(K)$, we can compute generators $E(K)/T$ by using *infinite descent* as described in [SIK95] or [Cre97, p.77]. This technique requires upper bounds on the height difference $h(P) - \hat{h}(P)$ over $E(K)$, and the efficiency of the process depends on having bounds that are as sharp as possible.

Suppose that $P_1, ..., P_r$ is a basis of $E(K)/T$, then the elliptic regulator of E/K is defined to be

$$R_{E/K} = \det\left(\langle P_i, P_j \rangle_{1 \leq i,j \leq r}\right),$$

which is an important term in the renowned Birch Swinnerton-Dyer conjecture. Therefore, numerical verification of the conjecture is heavily reliant on precise methods of computing the canonical height at points on $E(K)$, and requires computation of bases of $E(K)/T$ as discussed above. Moreover, the computation of $\hat{h}(P)$ and of bounds for $h - \hat{h}$ are also used in the computation of integral points $E(K)$.

Often the most suitable method of computation required for finding canonical heights or bounding the height difference depends on the specific elliptic curve, number field, and points that are being considered. It is therefore key to have numerous techniques that are applicable when different situations arise, and so we aim to present a variety of methods throughout.

This essay is divided into three parts, the first of which is dedicated to providing sufficient background for the subsequent sections, where we define naive and canonical heights, and prove results concerning the local decomposition of the canonical height.
In Part II of this essay, we present methods for computing the the canonical height of a point on an elliptic curve via the decomposition into local heights. Section 6 concerns the case of non-Archimedean places of K, and uses reduction theory to describe efficient algorithms for computing the local height, as well as methods for finding the *overall* non-Archimedean contribution to $\hat{h}(P)$. Section 7 then deals with local heights at Archimedean places, and we present two techniques of different flavour that can be implemented.
The final part of this essay is devoted to computing bounds of the difference $h(P) - \hat{h}(P)$ between the naive height and the canonical height. The strategy is again that of local decomposition, and in the non-Archimedean case, which is covered in Section 10, much of the theory overlaps with Section 7. Lastly, Section 11 concerns the Archimedean case of local height, where we again give competing methods for computation of bounds, each of which are suited to different computational purposes.

Part I
Preliminaries

In this part of the essay, we introduce the definitions of the naive and canonical height of a point on an elliptic curve defined over a number field, mainly following [Sil09] and [Sil94]. We will also prove some results which will be useful in later sections, and show that the canonical height may be decomposed into a sum of local heights. First we clarify some notation which, unless otherwise stated, is used throughout.

Let K be a number field, and let $\mathcal{O}_K$ be the ring of integers. We shall denote the set of places (or primes) on K by M_K, which can be separated into the set of non-Archimedean (or finite) places M_K^0, and the Archimedean (or infinite) places M_K^∞. For each place $v \in M_K$, we write K_v to denote the v-adic completion of K, $\mathcal{O}_v$ to be the valuation ring, and choose a standard absolute value defined as follows:

Let v be the finite place associated to the prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, and $\mathrm{ord}_v() : K_v^\times \twoheadrightarrow \mathbb{Z}$ the normalised valuation map for v. Define the standard absolute value for v to be

$$|\alpha|_\mathfrak{p} = |\alpha|_v = \big(\frac{1}{N(\mathfrak{p})}\big)^{\mathrm{ord}_\mathfrak{p}(\alpha)/n_v} \quad \text{for } \alpha \in K_v^\times,$$

with $n_v = [K_v : \mathbb{Q}_w]$, where w is the place of $\mathbb{Q}$ lying below v. In particular, we may invert the relation above to get

$$\mathrm{ord}_v(\alpha) = \frac{-n_v \log |\alpha|_v}{\log(\#k_v)},$$

where k_v is the residue field. This is a natural choice of absolute value, since given an extension of number fields L/K, and $\mathfrak{P} \mid \mathfrak{p}$, we have that $|\cdot|_\mathfrak{P}$ restricts to $|\cdot|_\mathfrak{p}$ on K.

For v an infinite place, there is a real embedding $\sigma : K \hookrightarrow \mathbb{R}$, or a complex conjugate pair of embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$ associated to v, and the standard absolute value is defined by

$$|\alpha|_v = |\sigma(\alpha)|_\infty,$$

where $|\cdot|_\infty$ is the usual inner product on $\mathbb{C}$.

2 The Naive Height

Let E be an elliptic curve defined over K with Weierstrass equation,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

Unless otherwise stated, we assume that all Weierstrass equations have the form above, with $a_i \in \mathcal{O}_K$. Also, define constants b_i, c_i and the discriminant Δ associated to the Weierstrass equation as follows,

$$\begin{aligned} b_2 =& a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \\ b_8 =& a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 =& b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta =& -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned} \tag{2.2}$$

Definition 2.1 Let E/K be an elliptic curve given by Weierstrass equation (2.1), the naive height is the map $h : E \to \mathbb{R}$ defined by

$$P \mapsto \begin{cases} \dfrac{1}{[K:\mathbb{Q}]} \displaystyle\sum_{v \in M_K} n_v \log(\max\{1, |x(P)|_v\}) & \text{if } P \neq \mathcal{O} \\ 0 & \text{if } P = O. \end{cases}$$

Note that this is a finite sum, and since the $x(P)$ depends on the given Weierstrass equation of E, then so too does the naive height. Moreover, if L/K is a finite extension of number fields, then given any $v \in M_K$ the extension formula

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K] n_v,$$

implies that the height of a point $P \in E$ is independent of the number field which it is defined relative to. We shall now quote the main properties of the naive height, which are proven in [Sil09, Chapter VIII];

Proposition 2.2 Let E/K be an elliptic curve with Weierstrass equation (2.1). For all $P, Q \in E$, we have

(i) Given any $m \in \mathbb{Z}$,

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

(ii)

$$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1),$$

where $O(1)$ denotes a function which is bounded by some constant depending only on the Weierstrass equation.

This essentially says that the naive height is 'almost' a quadratic form on E, which begs the question of whether we may modify the height such that it has more attractive properties, leading to the definition of the canonical height.

3 The Canonical Height

Let K be a number field, and E be an elliptic curve defined over K given by Weierstrass equation W.

Proposition 3.1 Given any $P \in E$, the limit

$$\lim_{n \to \infty} \frac{1}{4^n} h(2^n P)$$

exists.

Proof. We show that this is a Cauchy sequence, indeed for $m > n$ in $\mathbb{N}$,

$$\begin{aligned} \left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| &= \left| \sum_{i=n}^{m-1} \frac{1}{4^{i+1}} h(2^{i+1} P) - \frac{1}{4^i} h(2^i P) \right| \\ &\leq \sum_{i=n}^{m-1} \frac{1}{4^{i+1}} |h(2^{i+1} P) - 4h(2^i P)|, \end{aligned}$$

and by Proposition 2.2.(i) , there exists some constant C, depending only on the Weierstrass equation, such that for all $Q \in E$

$$|h(2Q) - 4h(Q)| \leq C.$$

Therefore we have

$$\left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| \leq \sum_{i=n}^{m-1} \frac{1}{4^{i+1}} C = \frac{C}{3 \cdot 4^n}$$

which tends to zero as n tends to infinity. □

This allows us to define the canonical height as follows,

Definition 3.2 The canonical height of a point $P \in E$ is defined to be

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{4^n} h(2^n P),$$

and again, we quote the essential properties of $\hat{h}$ where proofs can be found in [Sil09, Chpater VIII].

Theorem 3.3 The canonical height has the following properties:

(i) $\hat{h}$ is independent of our choice of Weierstrass equation

(ii) For any $m \in \mathbb{Z}$ and $P \in E$ we have
$$\hat{h}(mP) = m^2\hat{h}(P).$$

(iii) Given $P, Q \in E$,
$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(iv) $|h(P) - \hat{h}(P)|$ is bounded on E

(v) Suppose $\hat{g} : E \to \mathbb{R}$ is another function satisfying (iv), and (ii) for any single integer $m \in \mathbb{Z}$. Then $\hat{h} = \hat{g}$

Parts (ii) and (iii) of this theorem say that we have succeeded in producing a quadratic form on E, and so there is an associated bilinear form $\langle \cdot, \cdot \rangle : E \times E \to \mathbb{R}$ defined by

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

called the *Néron-Tate pairing* on E/K as discussed in the introduction. Part (iv) of the theorem will be studied in Part III of the essay, where we discuss how to compute bounds for $|h(P) - \hat{h}(P)|$ over $E(K)$.

4 Decomposition into local heights

The limit definition of $\hat{h}$ is not particularly well suited to computation, as we shall discuss in Part II. Instead, we seek a local decomposition of the canonical height,

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P), \tag{4.1}$$

for some functions $\lambda_v : E(K_v) \setminus \{O\} \to \mathbb{R}$.
To construct these functions, we'll begin by following the more concrete approach of [CPS06], and make this rigorous in accordance with the exposition of [Sil94, Chapter VI]. Note that there are various normalisations for λ_v that appear in the literature, our approach will be to adopt the normalisation in [CPS06] throughout for consistency, and (hopefully) clarity.

Let E/K be an elliptic curve defined by Weierstrass equation W as in (2.1), and let $v \in M_K$ be a place of K. The duplication formula is

$$x(2P) = \frac{g(P)}{f(P)},$$

where f, g are polynomials depending on W given by

$$\begin{aligned} f(P) &= 4x(P)^3 + b_2x(P)^2 + 2b_4x(P) + b_6, \\ g(P) &= x(P)^4 - b_4x(P)^2 - 2b_6x(P) - b_8. \end{aligned}$$

Prop/Definition 4.1 Let $\Phi_v : E(K_v) \to \mathbb{R}$ be the function

$$\Phi_v(P) = \begin{cases} 1 & \text{if } P = O \\ \dfrac{\max\{|f(P)|_v, |g(P)|_v\}}{\max\{1, |x(P)|_v^4\}} & \text{otherwise.} \end{cases}$$

This is continuous and bounded on $E(K_v)$ (which has the v-adic topology), and there exists a constant $c > 0$ such that

$$\forall P \in E(K_v), \;\; \Phi_v(P) \geq c.$$

In particular, $\log(\Phi_v)$ is also a continuous bounded function on $E(K_v)$.

Proof. Firstly, away from O we have Φ_v is a quotient of maxima of polynomials in $x(P)$ with non-zero denominator, hence is continuous. Taking limits as $P \to O$ gives $x(P) \to \infty$, thus $|x(P)|_v^4$ dominates the numerator and the denominator, and the limit is equal to 1. Moreover, $E(K_v)$ is compact in the $v-$adic topology, and so Φ_v being continuous implies that it is bounded.
For the second statement, observe that since Φ_v is continuous at O, there exists some $R \in \mathbb{R}$ such that if $|x(P)|_v \geq R$, then $\Phi_v(P) \geq \frac{1}{2}$. For the case where $|x(P)|_v \leq R$, by direct calculation one finds that $\text{Resultant}(f, g) = \Delta^2$ (cf. [Sil94, p.458]), where $\Delta \neq 0$ is the discriminant of W. Therefore f, g are coprime in $K_v[X]$. That is, there exist polynomials $S, T \in K_v[X]$ such that $f(X)S(X) + g(X)T(X) = 1$. Evaluating at $X = x(P)$ we gives

$$\begin{aligned} 1 &\leq |f(x)S(x) + g(x)T(x)|_v \\ &\leq 2\max\{|f(x)|_v, |g(x)|_v\} \cdot \max\{|T(x)|_v, |S(x)|_v\} \\ &\leq A\max\{|f(x)|_v, |g(x)|_v\}. \end{aligned}$$

for some $A > 0$. Putting this together, we have

$$\Phi_v(P) \geq \begin{cases} \dfrac{A}{\max\{1, R^4\}} & \text{for } x(P) \leq R \\ 1/2 & \text{for } x(P) \geq R, \end{cases}$$

which completes the proof. □

Now, notice that

$$\begin{aligned} h(2P) - 4h(P) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{|f(x)|_v, |g(x)|_v\} - \frac{4}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{|1|_v, |x(P)|_v\}, \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \Phi_v(P), \end{aligned} \tag{4.2}$$

assuming the second line converges. Hence the canonical height can be decomposed as follows

$$\begin{aligned} \hat{h}(P) &= \lim_{n \to \infty} \frac{1}{4^n} h(2^n P) \\ &= h(P) + \left(\frac{1}{4}h(2P) - h(P)\right) + \left(\frac{1}{4^2}h(4P) - \frac{1}{4}h(2P)\right) + \dots \\ &= h(P) + \frac{1}{[K:\mathbb{Q}]} \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \sum_{v \in M_K} n_v \log \Phi_v(2^i P) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \left(\log \max\{1, |x(P)|_v\} + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_v(2^i P) \right), \end{aligned}$$

if swapping of the summations is valid, and the sum $\sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log(\Phi_v(2^i P))$ converges. This motivates the following definition;

Definition 4.2 Let E/K be an elliptic curve with Weierstrass equation W. The local height $\lambda_v : E(K_v) \setminus \{O\} \to \mathbb{R}$ is defined to be

$$\lambda_v = \log \max\{1, |x(P)|_v\} + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_v(2^i P). \tag{4.3}$$

This is well defined by the following,

Proposition 4.3 The series

$$\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_v(2^i P)$$

converges to a continuous bounded function on $E(K_v)$.

Proof. It is a simple check to show that sum is absolutely and uniformly convergent on $E(K_v)$ by using the boundedness of $\log \Phi_v$, and since $\log \circ \Phi_v \circ [2^n]$ is continuous on $E(K_v)$ for all n, it follows that the series will be continuous also by uniform continuity. For boundedness again simply note that $E(K_v)$ is compact. □

Again, since the definitions of Φ_v, Ψ_v and λ_v depend on the f,g and the x-coordinate of P, they will a priori depend on the Weierstrass equation W.
We want to show that the local decomposition in equation (4.1) is actually correct. This requires the following theorem, which will be extremely useful in later sections.

Theorem 4.4 Let E/K be an elliptic curve with Weierstrass equation W, and let v be a non-Archimedean place on K. Suppose that W is minimal at v and let $P \in E_0(K_v)$, then

$$\Phi_v(P) = 1,$$

and in particular,

$$\lambda_v(P) = \log \max\{1, |x(P)|_v\}$$

Proof. Recall that $P = (x, y) \in E_0(K)$ if its reduction $\tilde{P}$ modulo v is a non-singular point on $\tilde{E}$. Taking partial derivatives of W, this holds if and only if

$$|2y + a_1x + a_3|_v \geq 1, \quad \text{or} \quad |3x^2 + 2a_2x + a_4 - a_1y|_v \geq 1. \tag{4.4}$$

Let $\alpha(P), \beta(P)$ denote the expressions within the respective absolute values above. To prove the theorem, we'll split into two cases:
(i) Suppose that $|x|_v > 1$, we have all $|a_i| \leq 1$ since W is v-integral, thus

$$|f(P)|_v = |4x^3 + b_2x^2 + 2b_4x + b_6|_v \leq |x|_v^3,$$
$$|g(P)|_v = |x^4 - b_4x^2 - 2b_6x - b_8|_v = |x|_v^4,$$

hence

$$\Phi_v(P) = \frac{\max\{|x|_v^3, |x|_v^4\}}{\max\{1, |x|_v^4\}} = \frac{|x|_v^4}{|x|_v^4} = 1.$$

(ii) If instead $|x|_v \leq 1$, then we must also have $|g(P)|_v \leq 1$ and $|f(P)|_v \leq 1$. Begin by observing that f, g can be written in terms of α, β, as is given in [Sil94, p. 472];

$$f(P) = \alpha(P)^2 \quad \text{and} \quad g(P) = \beta(P)^2 + \alpha(P)\gamma(P),$$

where γ is some polynomial in $O_v[X, Y]$, so $|\gamma(P)|_v \leq 1$.
Suppose that $|\alpha(P)|_v \geq 1$. The left hand identity then implies that $|f(P)|_v \geq 1$, and so

$$\Phi_v(P) = \frac{\max\{1, |g(P)|_v\}}{1} = 1.$$

Otherwise, by (4.4) we must have $|\alpha(P)|_v < 1$ and $|\beta(P)|_v \geq 1$. Then taking absolute values of $|g(P)|_v$ we have

$$|g(P)|_v = |\beta(P)^2 + \alpha(P)\gamma(P)|_v = 1,$$

and we can again conclude that $\Phi_v(P) = 1$. □

Remark: In fact the converse also holds, although we shall not prove this.

Corollary 4.5 Let E/K be an elliptic curve, with Weierstrass equation W. There exists a finite set $S \subset M_K$ such that for all $v \notin S$,

$$\lambda_v(P) = \log \max\{1, |x(P)|_v\}.$$

Proof. Let S be the set of all primes v where either

(i) v is an infinite prime,

(ii) $v \mid (\Delta(W))$.[1]

This is a finite set, and given $v \notin S$ the Weierstrass equation W is minimal at v with $E_0(K) = E(K)$. Therefore, by the previous theorem we have $\lambda_v(P) = \log \max\{1, |x(P)|_v\}$. □

Now, as $\hat{h}$ is a quadratic form, we may hope that this also holds for the local heights. Unfortunately this is not the case, however we do have the following duplication formula,

Lemma 4.6 The function $\lambda_v : E(K_v) \setminus \{O\} \to \mathbb{R}$ satisfies the following duplication law for all $P \neq O$ such that $2P \neq O$;

$$\lambda_v(2P) = 4\lambda_v(P) - \log |f(P)|_v. \tag{4.5}$$

which follows easily from the equation (4.3) defining λ_v. From this, we can verify that the decomposition of $\hat{h}$ in equation (4.1) is correct.

Theorem 4.7 The canonical height has the following decomposition into local heights,

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

Proof. Recall from Theorem 3.3 that $\hat{h}$ is the unique function F satisfying the properties:

$$|F(P) - h(P)| = O(1), \text{ and } F(2P) = 4F(P).$$

Let $F(P)$ be the expression on the right hand side of (4.1). For the first property, we have

$$F(P) - h(P) = \frac{1}{[K : \mathbb{Q}]} n_v \Bigg(\sum_{v \in M_K} \big(\max \log\{1, |x(P)|_v\} - \Psi_v(P) \big) - \sum_{v \in M_K} n_v \max \log\{1, |x(P)|_v\} \Bigg),$$

and by Corollary 4.5, there is a finite $S \subset M_K$ such that

$$F(P) - h(P) = \sum_{v \in S} n_v \Psi_v(P).$$

As Ψ_v is a bounded function, we deduce that this finite sum is bounded on $E(K)$.
The second part then follows from Lemma 4.6, since we have

$$\begin{aligned} F(2P) &= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(2P) \\ &= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \left(4\lambda_v(P) - \log |f(P)|_v\right) \\ &= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \left(4\lambda_v(P)\right) \text{ (Product formula)} \\ &= 4F(P). \end{aligned}$$

□

To finish this section, we quote [Sil94, Chapter VI, Theorem 3.1],

Theorem 4.8 Let E/K be an elliptic curve with Weierstrass equation W, where K is a local field with place v. There exists a *unique* function $\lambda_v : E(K) \setminus \{O\} \to \mathbb{R}$ such that

(i) λ_v is continuous on $E(K) \setminus \{O\}$ and bounded away from O,

(ii) $\lim_{P \to O}(\lambda_v(P) - \log |x(P)|_v)$ exists,

(iii) The duplication formula (4.5) holds.

[1] Recall that we're assuming W has coefficients in $\mathcal{O}_K$, if not, we can simply add to S the places where W isn't v-integral.

Moreover, the function[2]

$$\lambda_v'(P) = \lambda_v(P) - \frac{1}{6}\log|\Delta(W)|_v$$

is independent of the Weierstrass equation for E, and given L/K a finite extension with w a the place of L lying above v, we have for all $P \in E(K) \setminus \{O\}$

$$\lambda_v(P) = \lambda_w(P)$$

The hard part of proving this theorem is actually showing the existence of λ_v, which we've shown above, the rest is simple to verify. Immediately from this theorem we can deduce the following,

Corollary 4.9 Let W and W' be two Weierstrass equations for an elliptic curve E/K, and $\lambda_v^{(W)}$, $\lambda_v^{(W')}$ the corresponding local heights for $v \in M_K$, then for all $P \in E(K_v) \setminus \{O\}$,

$$\lambda_v^{(W)}(P) = \lambda_v^{(W')}(P) + \frac{1}{6}\log\left|\frac{\Delta(W)}{\Delta(W')}\right|_v$$

5 Elliptic Curves over $\mathbb{C}$

In sections 7 and 10 of this essay we will require some knowledge of the theory of elliptic curves defined over $\mathbb{C}$, so here we give a brief outline of results in [Sil09, Chapter VI] and [Sil94, Chapter I], so as to avoid having to repeat ourselves later on.

Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$ be a lattice, then we can define the Weierstrass functions on $\mathbb{C}$ associated to Λ as follows;

$$\begin{aligned}
\wp(z;\Lambda) &= \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2},\\
\sigma(z;\Lambda) &= z\prod_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(1-\frac{z}{w}\right) e^{z/\omega+(z/\omega)^2},\\
\zeta(z;\Lambda) &= \frac{\sigma'(z;\Lambda)}{\sigma(z;\Lambda)} = \frac{1}{z} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right),
\end{aligned}$$

and we define the 'quasi-periodic' function $\eta : \Lambda \to \mathbb{C}$ to be

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

which is independent of z. One can show [Sil09, Ch.VI, Theorem 3.5.(b)] that $\wp$ satisfies the differential equation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2(\Lambda)\wp(z;\Lambda) - g_3(\Lambda),$$

where g_2, g_3 are constants depending on the lattice. Hence, defining the elliptic curve $E_\Lambda/\mathbb{C}$ by $y^2 = 4x^3 - g_2x - g_3$, we have a map

$$\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C});\ \ z \mapsto (\wp(z;\Lambda), \wp'(z,\Lambda)), \tag{5.1}$$

which is an isomorphism of groups [Sil09, Ch.VI, Prop 3.6]. Moreover, the change of variables $y \mapsto 2y$ puts this in standard Weierstrass form as in equation (2.1)

$$W_\Lambda : y^2 = x^3 - \frac{1}{4}g_2(\Lambda) - \frac{1}{4}g_3(\Lambda). \tag{5.2}$$

Importantly, the *uniformisation theorem* [Sil09, Ch.VI, Theorem 5.1], says that an inverse to this construction exists. Given a Weierstrass equation W with coefficients in $\mathbb{C}$, a unique change of variables

[2] In fact, dividing this by two gives the normalisation for local height as in [Sil94].

$x = x' + r, y = y' + sx' + t$ puts gives a Weierstrass equation in shortened form W'.[3] There then exists a lattice $\Lambda \subset \mathbb{C}$ such that $W' = W_\Lambda$ as in equation (5.2).
Now, for any $\alpha \in \mathbb{C}^\times$, multiplication by α gives an isomorphism $\mathbb{C}/\Lambda \cong \mathbb{C}/(\alpha\Lambda)$. In particular, the Weierstrass equation W_Λ and $W_{(\alpha\Lambda)}$ will be isomorphic - that is, they are two Weierstrass equations for the same elliptic curve. Thus, given an elliptic curve $E/\mathbb{C}$ given by Weierstrass equation W, we may choose a lattice of the form $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, where $\mathrm{Im}(\tau) > 0$, such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$, but must be careful since the Weierstrass equation W_τ corresponding to Λ_τ may not have the same discriminant as our original equation W.

For a Weierstrass equation W, to find the periods ω_1, ω_2 and compute the inverse map to (5.1), one must integrate the invariant differential dx/y of the elliptic curve over certain paths . The details are omitted, although we shall use algorithms in order to find lattice periods and $z(P)$ in sections 7, 10.

Lastly, suppose that E/K is an elliptic curve with Weierstrass equation W, and v an infinite place of K. Then K_v is $\mathbb{R}$ or $\mathbb{C}$, so we may embed K into $\mathbb{C}$ and consider E as an elliptic curve defined over $\mathbb{C}$. Then [Sil94, Ch.VI, Theorem 3.2], gives an explicit formula for the local height at v,

$$\lambda_v(P) = -2\log|e^{-\frac{1}{2}z\eta(z;\Lambda)}\sigma(z;\Lambda)|.$$

which may be proven by showing that it satisfies (i),(ii) and (iii) in Theorem 4.8. An important subtlety is to remember that this normalisation of the local height is dependent on the Weierstrass equation, and hence on our choice of lattice. If Λ, Λ' are two period lattices corresponding to E, then we may use Corollary 4.9 to compare the local heights.

Part II
Computing Canonical heights on Elliptic curves

In this part of the essay, we'll discuss methods for calculating $\hat{h}(P)$ a point P on an elliptic curve E/K. The limit definition (3.2) of $\hat{h}(P)$ isn't practical for computation, since the values $h(2^nP)$ become extremely large, which is inefficient when working with computers. Instead, we exploit the theory of local heights developed in the previous sections in order to decompose the problem into computing $\lambda_v(P)$ for places $v \in M_K$.

6 Local height at Non-Archimedean Places

The aim of this section is to compute the non-Archimedean contribution $\hat{h}_0(P)$ of the canonical height. That is, the sum

$$\hat{h}_0(P) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^0} n_v\lambda_v(P) = h(P) - \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^0} n_v\Psi_v(P).$$

The results presented shall mainly follow [Sil88] and [MS16]. Silverman's method [Sil88, Section 5] gives a very fast way to compute $\lambda_v(P)$ when W is minimal at v, and if the factorisation of (Δ) is known then we can turn this into an efficient algorithm for computing $\hat{h}_0(P)$. On the other hand, the paper [MS16] provides an algorithm to compute $\lambda_v(P)$ when W is not minimal, which allows us to find $\hat{h}_0(P)$ without knowing the factorisation of (Δ). First, we need a brief digression on Kodaira symbols and Tate's algorithm.

6.1 Reduction Types

Let K be a *local field* with discrete non-Archimedean valuation v, valuation ring $\mathcal{O}$, and residue field k. Suppose that E/K is an elliptic curve defined by a minimal Weierstrass equation

$$W^{\min} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

[3] Importantly, this doesn't change the discriminant of the equation.

where $a_i \in \mathcal{O}$. Recall that the reduction of E modulo v is the curve $\tilde{E}/k$, which is defined by reducing $W^{\min}$ modulo v. There are three broad cases for the type of reduction:

(i) $\tilde{E}$ is non-singular; $v(\Delta) = 0$ (good reduction),

(ii) $\tilde{E}$ is singular, and the singular point is a node; $v(\Delta) > 0, c_4 = 0$ (multiplicative reduction),

(iii) $\tilde{E}$ is singular, and the singular point is a cusp; $v(\Delta) > 0, c_4 > 0$ (additive reduction).

Moreover, the multiplicative case is said to be *split* if the polynomial $f(X) = X^2 + a_1X - a_2$ splits in k, and is called *non-split* otherwise. It is clear that by taking a finite unramified extension L/K, we may pass from the non-split case to the split case.

However, there are more refined ways to classify the reduction type of E, and by using methods from intersection theory, one arrives at the notion of the *Kodaira symbol* of $\tilde{E}/k$. The Kodaira symbol of $\tilde{E}$ gives useful information about the elliptic curve, as summarised in Table 1 below, which is taken from [Sil94, p.365]. The types I_0 and I_m correspond to good and multiplicative reduction respectively, while all other types are additive.

Kodaira Type	Tamagawa index c		$E(K)/E_0(K)$
	$k = k'$	$k \neq k'$	
I_0	1	1	(0)
I_m, m even	m	2	$\mathbb{Z}/m\mathbb{Z}$
I_m, m odd	m	1	$\mathbb{Z}/m\mathbb{Z}$
III	2	2	$\mathbb{Z}/2\mathbb{Z}$
IV	3	1	$\mathbb{Z}/3\mathbb{Z}$
I_0^*	4	1 or 2	$(\mathbb{Z}/2\mathbb{Z})^2$
I_m^*, m even	4	2	$(\mathbb{Z}/2\mathbb{Z})^2$
I_m^*, m odd	4	2	$\mathbb{Z}/4\mathbb{Z}$
IV*	3	1	$\mathbb{Z}/3\mathbb{Z}$
III*	2	2	$\mathbb{Z}/2\mathbb{Z}$

Table 1: Table of Kodaira symbols and Tamagawa indices, the final column gives the component group in the case where $k = k'$, where k' is the splitting field of a polynomial as in [Sil94, p.365-8].

The method of finding the Kodaira type is called *Tate's algorithm*, which we will occasionally have to reference, and is described in [Sil94, p.365-8]. Note that in Silverman's book the table assumes that k is algebraically closed, however in the general case the Tamagawa index depends on whether certain polynomials split in the residue field, as described in his description of Tate's algorithm. As with the case of split/non-split multiplication, we can pass to an unramified extension L/K such that the relevant polynomial splits in k_L, and we have an injection

$$E(K)/E_0(K) \hookrightarrow E(L)/E_0(L),$$

where the component group $E(L)/E_0(L)$ is described in Table 1.

6.2 Silverman's Algorithm

Let K be a number field, E/K an elliptic curve with Weierstrass equation W. Suppose that we know the factorisation of the discriminant $\Delta(W)$, then for any finite prime v not dividing (Δ), the curve has good reduction at v. Therefore, by Theorem 4.4 the local height is $\lambda_v(P) = \log \max\{1, |x(P)|_v\}$, and we have

$$\begin{aligned}\hat{h}_0(P) &= \sum_{v|(\Delta)} \lambda_v(P) + \sum_{v\nmid(\Delta)} \log \max\{1, |x(P)|_v\}, \\ &= \sum_{v|(\Delta)} \lambda_v(P) + \sum_{\substack{v\nmid\Delta \\ |x|_v>1}} \log |x(P)|_v.\end{aligned}$$

In particular, the set of primes dividing (Δ), and the set of primes v such that $v \nmid (\Delta)$ and $|x|_v > 1$ are both finite, so computing $\hat{h}_0(P)$ only requires us to consider finitely many $v \in M_K^0$. Our goal is therefore to compute $\lambda_v(P)$ as efficiently as possible.

Let $v \in M_K^0$ be a finite place of K, then K_v is a local field as in the previous section. To use the reduction theory, one needs a *minimal* Weierstrass equation at v, hence the first task is to find such an equation. There are many methods to do so, for example Tate's Algorithm for computing (among other things) the Kodaira symbol of E/K_v will produce a minimal equation once terminated. However, there are more efficient methods, such as that in [Las82, Section 2] which can be modified for computing locally minimal equations. Finding the minimal equation of an elliptic curve at a fixed place v is a relatively fast procedure, indeed using Laska's algorithm will require less than or equal to $\max\{\mathrm{ord}_v(c_4), \mathrm{ord}_v(c_6)\}$ iterations, where each iteration involves finitely many computations.
If we can compute the local height at P with respect to a minimal Weierstrass equation W', then recalling Corollary 4.9 we can compute the local height with respect to W via,

$$\lambda_v^{(W)}(P) = \lambda_v^{(W')}(P) + \frac{1}{6}\log\left|\frac{\Delta(W)}{\Delta(W')}\right|_v.$$

For the remainder of this section, we shall assume that E/K is defined by a Weierstrass equation W minimal at v, with coefficients a_i, and the usual constants defined as in (2.2). Firstly, we have a proposition which will be key to the method discussed.

Proposition 6.1 With the notation above, suppose that $P \in E(K_v) \setminus \{O\}$, then

(i) If $P \notin E_0(K_v)$, then $\lambda_v(P)$ depends only on the image of P in the component group $E(K_v)/E_0(K_v)$

(ii) If $P \in E_0(K_v)$, then $\lambda_v(P) = \log\max\{1, |x(P)|_v\}$

(iii) If E has split multiplicative reduction at v, and $P \notin E_0(K_v)$ lies in the ith component of $\mathbb{Z}/n\mathbb{Z} \cong E(K_v)/E_0(K_v)$, where $0 < i < n$, then

$$\lambda_v(P) = \frac{i(n-i)}{n^2}\log|\Delta|_v = -\frac{i(n-i)}{n}\frac{\log \#k_v}{n_v} \tag{6.1}$$

Proof. (ii) is just Theorem 4.4, while we omit (i),(ii). These are significantly harder to prove, and require the theory of Tate curves, which is the analogue of uniformisation for p-adic fields. □

Now, given a point $P = (x, y) \in E(K_v)$ we would like to know whether P is in $E_0(K_v)$, since Proposition 6.1(ii) says that such points have a simple formula for local height. Well, the point $\tilde{P} \in \tilde{E}$ is non-singular if and only if the partial derivatives of W don't simultaneously vanish at $\tilde{P}$ in the residue field. That is,

$$P \in E_0(K_v) \iff \mathrm{ord}_v(3x^2 + 2a_2x + a_4 - a_1y) \leq 0 \quad \text{or} \quad \mathrm{ord}_v(2y + a_1x + a_3) \leq 0. \tag{6.2}$$

This gives us a simple way to check if P is a point of good reduction, and if so we can easily calculate the local height $\log\max\{1, |x(P)|_v\}$.

Next suppose that $P \notin E_0(K_v)$, and that E has split[4] multiplicative reduction, which happens when $\mathrm{ord}_v(\Delta) > 0$, $\mathrm{ord}_v(c_4) = 0$, and $X^2 + a_1X - a_3$ splits in k_v. Then $E(K_v)/E_0(K_v) \cong \mathbb{Z}/n\mathbb{Z}$, where $n = \mathrm{ord}_v(\Delta)$, and we'd like to use equation (6.1) from the proposition to calculate the local height. Thus, given $P \notin E_0(K_v)$, we want to compute which component of $\mathbb{Z}/n\mathbb{Z}$ it belongs to, hence the following proposition from [Sil88, Prop 5.1],

Proposition 6.2 Let $P \in E(K_v)\backslash E_0(K_v)$, and suppose that P lies in the ith component of $E(K_v)/E_0(K_v)$, with $0 < i \leq n/2$, then

$$i = \min\left\{\mathrm{ord}_v(2y + a_1x + a_3), \frac{\mathrm{ord}_v(\Delta)}{2}\right\} \tag{6.3}$$

[4]The non-split case is slightly subtle, which we come to in a moment.

Proof. Suppose that $i \neq n/2$, so $2P \notin E_0(K_v)$, and recall the duplication formula for local heights is

$$\lambda_v(2P) = 4\lambda_v(P) - \log|f(P)|_v.$$

We can substitute P and $2P$ into equation (6.1), and get that

$$\frac{2i(n-2i)}{n^2}\log|\Delta|_v = \frac{4i(n-i)}{n^2}\log|\Delta|_v - \log|f(P)|_v,$$

which rearranges to give

$$i = \frac{n\log|f(P)|_v}{2\log|\Delta|_v} = \frac{1}{2}\mathrm{ord}_v(f(P)) = \mathrm{ord}_v(2y + a_1x + a_3)$$

where the equalities use the fact that $\mathrm{ord}_v(\alpha) = -\frac{n_v \log|\alpha|_v}{\log \# k_v}$ for all $\alpha \in K_v^\times$, and $f(P) = (2y + a_1x + a_3)^2$.

If instead we have $i = n/2$, then $2P$ has good reduction, so $\lambda(2P) = \log\max\{1, |x(P)|_v\} \geq 0$. Hence

$$0 \leq \lambda_v(2P) = 4\lambda_v(P) - \log|f(P)|_v = \frac{4}{n^2}\left(\frac{n}{2}\right)^2\log|\Delta|_v - \log|f(P)|_v,$$

and again using the relation between $\mathrm{ord}_v(\cdot)$ and $|\cdot|_v$ we deduce by rearranging that

$$\mathrm{ord}_v(2y + a_1x + a_3) \geq \frac{1}{2}\mathrm{ord}_v(\Delta) = \frac{n}{2}$$

□

Suppose instead that $P \in E(K_v) \setminus E_0(K_v)$ lies in the ith component with $n/2 < i < n$. Then since equation (6.3) is invariant under $P \mapsto -P$, which corresponds to the map $i \mapsto (n-i)$ in $E(K_v)/E_0(K_v)$, we have that (6.3) is equal to $(n-i)$ as opposed to i. However, the equation for local height

$$\lambda_v(P) = \frac{i(n-i)}{n^2}\log|\Delta|_v = -\frac{i(n-i)}{n}\frac{\log \# k_v}{n_v}$$

is *also* invariant under the map $i \mapsto (n-i)$. Therefore, if we calculate $\lambda_v(P)$ using the equation above, where i is obtained from equation (6.3), then we get the correct result even if $n/2 < i < n$.

In the case of non-split multiplicative reduction, again let $n = \mathrm{ord}_v(\Delta)$, then Table 1 says that the Tamagawa index is either 1 for n odd, or 2 when n is even. Hence in general $E(K_v)/E_0(K_v) \ncong \mathbb{Z}/n\mathbb{Z}$, and the discussion of being in the ith component above doesn't really make sense. However, we can let L be an unramified extension of K_v such that E has split multiplicative reduction over L, and let w be the place above v on L. Then $\mathrm{ord}_w = \mathrm{ord}_v$ on $K_v^\times$, and from Theorem 4.8 we know that $\lambda_v = \lambda_w$ on $E(K_v)$. Hence for $P \in E(K_v) \setminus E_0(K_v)$ we have

$$\lambda_v(P) = \lambda_w(P) \overset{(6.1)}{=} \frac{i(n-i)}{n^2}\log|\Delta|_w = \frac{i(n-i)}{n^2}\log|\Delta|_v,$$

where i is given by the equation

$$i = \min\left\{\mathrm{ord}_w(2y + a_1x + a_3), \frac{\mathrm{ord}_w(\Delta)}{2}\right\} = \min\left\{\mathrm{ord}_v(2y + a_1x + a_3), \frac{\mathrm{ord}_v(\Delta)}{2}\right\}.$$

However this is *exactly* the same as the computation in the split multiplicative case, meaning we don't have to discern between the split and non-split cases for multiplicative reduction when calculating $\lambda_v(P)$.

The remaining case is that of additive reduction, for which we shall need the classification by Kodaira symbol from the previous section. First, define the following two polynomials

$$\psi_2(P) = 2y + a_1x + a_3,$$
$$\psi_3(P) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$

which square to the denominators of $x(2P)$ and $x(3P)$ respectively. The local height satisfies duplication (recall Lemma 4.6) and triplication[5] formulae

$$\lambda_v(2P) = 4\lambda_v(P) - 2\log|\psi_2(P)|_v,$$
$$\lambda_v(3P) = 9\lambda_v(P) - 2\log|\psi_3(P)|_v.$$

If $P \in E(K_v) \setminus E_0(K_v)$, then the Tamagawa index c_v must be greater than one. We recall Table 1 below, having removed cases where $c_v = 1$ and the those that we've already covered, and so deduce that the reduction $\tilde{E}$ modulo v has Kodaira symbol III, IV, I_m^*, IV* or III*.

Kodaira Type	Tamagawa index c	$E(K)/E_0(K)$
III	2	$\mathbb{Z}/2\mathbb{Z}$
IV	3	$\mathbb{Z}/3\mathbb{Z}$
I_m^*, m even	4 or 2	$(\mathbb{Z}/2\mathbb{Z})^2$ or $\mathbb{Z}/2\mathbb{Z}$
I_m^*, m odd	4 or 2	$\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$
IV*	3	$\mathbb{Z}/3\mathbb{Z}$
III*	2	$\mathbb{Z}/2\mathbb{Z}$

There are then 3 cases to consider:
(i) Suppose $3P \in E_0(K_v)$, then by inspecting the table above, $\tilde{E}$ must have Kodaira symbol IV or IV*, and P and $-2P$ have the same image in the quotient $\frac{E(K_v)}{E_0(K_v)}$. Thus by Proposition 6.1, we have $\lambda_v(P) = \lambda_v(-2P)$. But λ_v depends only on the x-coordinate of P, hence $\lambda_v(P) = \lambda_v(-P)$, and so in this case we must have

$$\lambda_v(P) = \lambda_v(2P) = 4\lambda_v(P) - 2\log|\psi_2(P)|_v,$$

which rearranges to give

$$\lambda_v(P) = \frac{2}{3}\log|\psi_2(P)|_v.$$

Moreover, since $3P$ has good reduction, the formula for local height implies that $\lambda_v(3P) \geq 0$, which we can substitute into the triplication formula to deduce that

$$\lambda_v(P) = \frac{2}{3}\log|\psi_2(P)|_v \geq \frac{2}{9}\log|\psi_3(P)|_v.$$

(ii) If instead $2P \in E_0(K_v)$, then the reduction has type III,III* or I_m^*. By the same approach, noting that $2P \in E_0(K_v)$ and $\lambda_v(P) = \lambda_v(3P)$ (since they have the same image in the quotient) we find that

$$\lambda_v(P) = \frac{1}{4}\log|\psi_3(P)|_v \geq \frac{1}{2}\log|\psi_2(P)|_v.$$

Importantly, the inequalities in cases (i) and (ii) cannot both hold.
(iii) Lastly suppose that neither (i) nor (ii) holds. Then by consulting our table one finds that the curve has reduction type I_m^*, where m is odd, and the quotient group is $E(K_v)/E_0(K_v) \cong \mathbb{Z}/4\mathbb{Z}$. So we gather that $-3P$ and P have the same image, and thus

$$\lambda_v(P) = \frac{1}{4}\log|\psi_3(P)|_v.$$

The pressing question now is whether there is a way to distinguish this from the cases (i) and (ii) without having to actually compute the Kodaira symbols. It follows from Tate's algorithm that in this case, *neither* of the inequalities in cases (i) and (ii) hold - hence by checking through the two inequalities, we can determine the local height for a curve with additive reduction.

The discussion above proves the validity of an algorithm to compute $\lambda_v(P)$, which is summarised below:

[5]Showing this is non-trivial, and is relevant to the paper [Uch08] which we discuss briefly in Section 10. To prove it one may follow [Sil94, Ch. VI Ex 6.3-4], although we do not have space to do so here.

Algorithm 1 Let E/K be an elliptic curve with Weierstrass equation W, minimal at v. Compute the local height $\lambda_v(P)$ for a point $P = (x, y) \in E(K_v)$ as follows,

1. (Good reduction) Compute

$$\mathrm{ord}_v(3x^2 + 2a_2x + a_4 - a_1y) \quad \text{and} \quad \mathrm{ord}_v(2y + a_1x + a_3),$$

   if either is less than or equal to zero, return $\lambda_v(P) = \log \max\{1, |x|_v\}$.

2. (Multiplicative reduction) Otherwise, if $\mathrm{ord}_v(c_4) = 0$ then set $n = \mathrm{ord}_v(\Delta)$, and $i = \min\{\mathrm{ord}_v(2y + a_1x + a_3), n/2\}$, and return

$$\lambda_v(P) = -\frac{i(n-i)}{n}\frac{\log \#k_v}{n_v}.$$

3. (Additive reduction) Otherwise,

   (a) If $\mathrm{ord}_v(\psi_3(P)) \geq 3\mathrm{ord}_v(\psi_2(P))$, then we're in case (i) above, so return

$$\lambda_v(P) = \frac{2}{3}\log|\psi_2(P)|_v. \qquad \text{(Types IV or IV}^*\text{)}$$

   (b) Otherwise, we're in case (ii) or (iii) above, hence return

$$\lambda_v(P) = \frac{1}{4}\log|\psi_3(P)|_v. \qquad \text{(Types III, III}^*\text{ or I}_m^*\text{)}$$

6.3 Müller-Stoll Algorithm

The method discussed above is very fast when we already know the factorisation of (Δ) into prime ideals. However, if we don't know, or cannot compute this factorisation, then we're left with the daunting task of computing $\lambda_v(P)$ for *all* non-Archimedean places, so computing them individually is of little use. Indeed, knowing the prime factors of (Δ) gives the prime factors of $\mathcal{N}(\Delta)$, hence a factorisation algorithm for (Δ) has complexity at least as bad as factoring $\mathcal{N}(\Delta)$ over $\mathbb{Z}$, which is no easy feat.

In this section, we present a method from [MS16] to compute $\hat{h}_0(P)$ when $K = \mathbb{Q}$, that does not require a factorisation of (Δ), and discuss how one may generalise to other number fields. To begin, we need a method of computing $\lambda_v(P)$ when the Weierstrass equation W is not minimal at v. Recall that

$$\lambda_v(P) = \log \max\{1, |x(P)|_v\} - \Psi_v(P),$$

and following the notation of Muller/Stoll, we define

$$\mu_v(P) = \frac{n_v}{\log \#k_v}\Psi_v(P).$$

First, we shall present [CPS06, Proposition 6], which elaborates on results from the previous section, and allows us to read off possible values of μ_v given the Kodaira symbol for reduction modulo v;

Proposition 6.3 Let E/K be an elliptic curve with Weierstrass equation W which is minimal at $v \in M_K^0$ and suppose E has Tamagawa index $c_v > 1$. Then for $P \notin E_0(K_v)$ we have

$$\lambda_v(P) = -\Psi_v(P),$$

and the possible values of $\mu_v(P)$ are recorded in the table below, as well as corresponding upper bounds α_v.

Proof. The first statement in the proposition is equivalent to saying that $|x(P)|_v \leq 1$, which must hold for all $P \notin E_0(K_v)$, since if $|x(P)|_v > 1$, then P reduces the the point at infinity on the reduced curve, which is a non-singular point (ie. $P \in E_1(K_v) \subset E_0(K_v)$).
Now suppose $P \notin E_0(K_v)$, we can then use Silverman's algorithm to calculate $\lambda_v(P)$ in terms of the

Kodaira Type	Tamagawa index c_v	$\mathrm{ord}_v(\Delta)$	μ_v	α_v
Any	1	-	0	0
I_m, $m \geq 2$	m	m	$i(m-i)/m, i = 1, ..., m-1$	$m/4$
I_m, $m \geq 2$ even	2	m	$m/4$	$m/4$
III	2	≥ 3	$1/2$	$1/2$
IV	3	≥ 4	$2/3$	$2/3$
I_0^*,	4 or 2	≥ 6	1	1
I_m^*	4	$\geq 6+m$	1	1
I_m^*	2	$\geq 6+m$	1, $(m+4)/4$	$(m+4)/4$
IV^*	3	≥ 8	$4/3$	$4/3$
III^*	2	≥ 9	$3/2$	$3/2$

Table 2: Possible values of $\mu_v(P)$ for points of bad reduction, and corresponding upper bounds α_v, given a minimal Weierstrass equation of E/K.

order of small polynomials in a_i and $x(P)$. The multiplicative result is the same as given in the previous section, and to get the values for the additive cases one must work through Tate's algorithm and use the conditions that arise on $\mathrm{ord}_v(a_i)$ and $\mathrm{ord}_v(b_i)$ to calculate the exact value of $\mathrm{ord}_v(\psi_2(P))$ or $\mathrm{ord}_v(\psi_3(P))$. The proof is given in [CPS06] but is not particularly illuminating. We include one case, where the Kodaira type is III, for a flavour of the result.

Suppose that P is a point of bad reduction, then making substitutions $x = x'+r$ and $y = y'+sx'+t$, where $r, s, t \in \mathcal{O}_v$, the minimality of the Weierstrass equation is unaffected, and the local height is unchanged by Corollary 4.9, as the discriminant of our new Weierstrass is the same as the original one. Thurs we can without loss of generality assume that $P = (0, 0)$, which greatly simplifies things in Silverman's algorithm, as

$$\begin{aligned}\mathrm{ord}_v(\psi_2(P)) &= \mathrm{ord}_v(2y + a_1x + a_3) = \mathrm{ord}_v(a_3),\\ \mathrm{ord}_v(\psi_3(P)) &= \mathrm{ord}_v(3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8) = \mathrm{ord}_v(b_8).\end{aligned}$$

Assuming that the reduction type is III, and working through Tate's algorithm as presented in [Sil94, p.366-8], we find

$$a_6 = 0, \qquad \pi \mid b_2, \qquad \pi^2 \mid b_6, \qquad \pi^2 \mid b_2, \qquad \pi^3 \nmid b_8,$$

and in Algorithm 1, we're in case (b), so

$$\mu_v(P) = \frac{1}{4}\mathrm{ord}_v(\psi_3(P)) = \frac{1}{4}\mathrm{ord}_v(b_8) = \frac{1}{2}.$$

We can then repeat this type of argument for different Kodaira symbols to fill the table. □

The table tells us that μ_v is a rational number for minimal Weierstrass equations, and the following proposition from [CPS06] allows us to use the results above for non-minimal Weierstrass equations.

Proposition 6.4 Let E/K be an elliptic curve, and let v be in M_K^0. Suppose E is given by a v-integral Weierstrass equation W, which is not necessarily minimal. We have

$$\inf_{P \in E(K_v)} \Psi_v(P) = 0,$$

attained at some $P \in E_0(K_v)$, and

$$\sup_{P \in E(K_v)} \Psi_v(P) = \left(\alpha_v + \frac{1}{6}\mathrm{ord}_v\left(\frac{\Delta}{\Delta^{\min}}\right)\right)\frac{\log \#k_v}{n_v}, \tag{6.4}$$

where α_v is as given in Table 2 , and $\Delta^{\min}$ is the discriminant of a minimal Weierstrass equation for E at v.

Proof. Suppose W' is a minimal Weierstrass equation for E at v, which is attained by the change of variables $x = u^2x' + r, y = u^3y' + u^2sx' + t$, where $\mathrm{ord}_v(u) \geq 1$ and $r, s, t \in \mathcal{O}_v$. Then Corollary 4.9 describes how λ_v acts under changing Weierstrass equation, from which we deduce that

$$\Psi_v(P) = \Psi'_v(P) + \log\left(\frac{\max\{1, |u^2x' + r|_v\}}{\max\{1, |x'|_v\}}\right) - \frac{1}{6}\log\left|\frac{\Delta}{\Delta^{\min}}\right|_v. \tag{6.5}$$

Now, we know from Theorem 4.4 that $\Psi'_v(P) = 0$ for all $P \in E_0(K_v)$, and for a v-integral equation one can show that Ψ_v is a non-negative function, hence $\inf_{P\in E(K_v)} \Psi_v(P) = 0$. The upper bounds of the table exactly say that $\sup_{P\in E(K_v)} \Psi'_v(P) = \alpha_v(\log \#k_v)/n_v$. Consider the middle term on the right hand side of equation (6.5). If $|x'| \leq 1$, which includes all cases of bad reduction, it is equal to zero, so

$$\Psi_v = \Psi'_v - \frac{1}{6}\log\left|\frac{\Delta}{\Delta^{\min}}\right|_v.$$

If $|x'|_v \geq 1$, we have good reduction, and the term inside the logarithm is

$$\frac{\max\{1, |u^2x' + r|_v\}}{|x'|_v} = \begin{cases} |u|_v^2 & |x'|_v \geq |u|_v^{-2} \\ \dfrac{1}{|x'|_v^2} & \text{otherwise} \end{cases}$$

Hence the infimum of the middle term is $\log |u|_v^2 = \frac{1}{6}\log|\Delta/\Delta^{\min}|_v$, which is attained for $|x'|_v$ sufficiently large, while the supremum is 0, and is attained[6] for $|x'|_v \leq 1$. The infimum/supremum of $\Psi'_v(P)$ is attained on the same domains of x, hence the infimum/supremum of $\Psi_v(P)$ is simply equal to their sum, which completes the proof. □

One should note also that multiplying equation (6.5) by $n_v/\log \#k_v$ implies that $\mu_v(P)$ is a rational number for all Weierstrass equations.

Now, define the function ε_v as

$$\varepsilon_v(P) = -\frac{n_v}{\log \#k_v}\log \Phi_v(P) = \min\{\mathrm{ord}_v(f(P)), \mathrm{ord}_v(g(P))\} - 4\min\{0, \mathrm{ord}_v(x)\},$$

which allows us to write μ_v as a series

$$\mu_v(P) = \sum_{i=0}^{\infty} \frac{1}{4^{i+1}}\varepsilon_v(2^iP).$$

Observing that K_v is the field of fractions of its integer ring $\mathcal{O}_v$, given $\alpha \in K_v$ we may write $\alpha = x_1/x_2$ for some elements $x_1, x_2 \in \mathcal{O}_v$. Moreover, we shall say that x_1/x_2 is *reduced* mod v if $\min\{\mathrm{ord}_v(x_1), \mathrm{ord}_v(x_2)\} = 0$. Suppose that $P \in E(K_v)$, and that $x(P) = \frac{x_1}{x_2}$ with $x_i \in \mathcal{O}_v$. Then we have $x(2P) = \frac{x'_1}{x'_2}$, where $x'_1 = x_2^4 g(P)$, and $x'_2 = x_2^4 f(P)$ are both v-integral. Moreover, substituting this into the equation for ε_v, we find

$$\varepsilon_v(P) = \min\{\mathrm{ord}_v(x'_1), \mathrm{ord}_v(x'_2)\} - 4\min\{\mathrm{ord}_v(x_1), \mathrm{ord}_v(x_2)\}.$$

In particular, if $\frac{x_1}{x_2}$ is reduced, then $\varepsilon_v(P) = \min\{\mathrm{ord}_v(x'_1), \mathrm{ord}_v(x'_2)\} \geq 0$.

Our current aim is to calculate $\mu_v(P)$, so consider the following lemmas,

Lemma 6.5 Let E/K be an elliptic curve with integral Weierstrass equation W, and $v \in M_K^0$ a finite place of K. Then for any $P \in E(K_v)$, we have

$$\varepsilon_v(P) = 0 \implies \varepsilon_v(2P) = 0.$$

[6] I suppose we should note that there *is* $P \in E(K_v)$ with $|x'|_v$ sufficiently large, which will follow from Hensel's lemma.

Proof. In the case where W is minimal at v, this follows from Theorem 4.4 and the remark after it, which says that $\varepsilon_v(P) = 0$ if and only if P is of good reduction. Suppose instead that W is not minimal.
If $|x(P)|_v > 1$, then it is simple to show that $\varepsilon_v(P) = 0$ and $|x(2P)|_v > 1$, so the result follows. The remaining case is where $\varepsilon_v(P) = 0$, $|x(P)|_v \leq 1$ and $|x(2P)|_v \leq 1$. Letting W' be a minimal Weierstrass equation for E/K, then the proof of the previous proposition says that for $u = \Delta/\Delta'$,

$$\mu_v(P) = \mu'_v(P) + 2\mathrm{ord}_v(u),$$
$$\mu_v(2P) = \mu'_v(2P) + 2\mathrm{ord}_v(u),$$

hence, using the fact that $\varepsilon_v(P) = 4\mu_v(P) - \mu_v(2P)$, we have

$$\varepsilon'_v(P) = \varepsilon_v(P) - 6\mathrm{ord}_v(u) = -6\mathrm{ord}_v(u) < 0,$$

which is a contradiction as $\varepsilon'_v(P) \geq 0$. Hence this case cannot arise when $\varepsilon_v(P) = 0$. □

This lemma shows that if $\varepsilon_v(P) = 0$, then $\mu_v(P) = 0$, which is useful, especially later on when proving Algorithm 3.

Lemma 6.6 Let v be a finite place in M_K^0, and E/K be an elliptic curve with v-integral Weierstrass equation W. Suppose that there are $M, B \in \mathbb{Z}_{\geq 0}$, with $M \geq 2$ such that

(i) $M'\mu_v(P) \in \mathbb{Z}$ for some $0 < M' \leq M$. That is, $\mu_v(P)$ has denominator bounded by M,

(ii) $\varepsilon_v(P)$ is bounded above by B on $E(K_v)$,

then letting $m = \lfloor \log(M^2B/3)/\log 4 \rfloor$, we have $\mu_v(P)$ is the unique fraction of denominator $\leq M$ in the interval $[\mu_0, \mu_0 + 1/M^2]$, where

$$\mu_0 = \sum_{0 \leq n \leq m} \frac{1}{4^{n+1}} \varepsilon(2^n P),$$

which follows simply by bounding the remainder of the sum, and noting that exactly one rational number with denominator bounded by M in any interval of length $1/M^2$.

From the bounds in Table 2, along with Proposition 6.4, we deduce that $\Delta(W)$ is a suitable candidate for both M and B. Hence Lemma 6.6 implies that following Algorithm computes $\mu_v(P)$:

Algorithm 2 Let π be a uniformiser of K_v,

1. Set $B = \mathrm{ord}_v(\Delta)$
2. If $B \leq 1$, return 0. Otherwise let $m = \lfloor \log(B^3/3)/\log(4) \rfloor$.
3. Compute μ_0 as follows: First set μ_0 and let $x(P) = \frac{x_1}{x_2}$ be a reduced fraction mod v, where x_i are computed to $(m+1)B + 1$ v-adic digits of precision.
4. For $n := 0$ to m:
   (a) Compute $x'_1 = x_2^4 g(P)$ and $x'_2 = x_2^4 f(P)$ to $(m+1)B + 1$ v-adic digits of precision
   (b) Set $l = \min\{\mathrm{ord}_v(x'_1), \mathrm{ord}_v(x'_2)\}$
   (c) Set $\mu_0 = \mu_0 + \frac{1}{4^{n+1}} l$
   (d) Set $x_i = \pi^{-l} x'_i$
5. Return the unique fraction in $[\mu_0, \mu_0 + 1/B^2]$ with denominator bounded by B

Proof. If $B \leq 1$, then W is minimal, and E has Tamagawa index 1, hence $\mu_v(P) = 0$. Otherwise the algorithm's validity follows from the previous lemma. Now, suppose that x_1/x_2 is reduced and x_i are known to N v-adic digits, where elements are stored as truncated power series in π. Then x'_1, x'_2 are also known to N v-adic digits, and have common factor π^l, where $\varepsilon_v(P) = l$. Hence by clearing the common factor to get our new values of x_1, x_2, we lose $l = \varepsilon_v(P)$ digits of precision. Now, for any $y \in O_v$, in order

to calculate $\mathrm{ord}_v(y)$, we only need to know y to *one* v-adic digit, since $\mathrm{ord}_v(y)$ is the index of the smallest non-zero term in the power series of y. Hence, for the algorithm to work, we at least need to know x_1, x_2 to one v-adic digit after $m+1$ iterations of the loop in step 4. By lemma 6.6, ε_v is bounded by B, so the loss of precision is bounded above by $B(m+1)$, and initially calculating x_1, x_2 to $B(m+1)+1$ digits of precision ensures that the algorithm is correct. □

So, how may we implement this method of computing $\mu_v(P)$ in order to compute the *overall* non-Archimedean contribution $\hat{h}_0(P)$ of the canonical height? We shall restrict ourselves to the more familiar case where $K = \mathbb{Q}$, then discuss possible ways to generalise afterwards. The idea is that we may group data about all primes at once by computing gcd's, which can be done in $\mathbb{Z}$ using Euclid's algorithm.

Let $E/\mathbb{Q}$ be an elliptic curve with integral Weierstrass equation W, and $P \in E(\mathbb{Q})$, we have

$$\hat{h}_0(P) = h_0(P) - \sum_p \Psi_p(P) = h_0(P) - \sum_p \mu_p(P)\log p,$$

and define $\Psi_0(P) = \sum_{v\in M_K^0} \Psi_v(P) = \sum_p \mu_p(P)\log p$. Suppose that $x(P) = x_1/x_2$ with $\gcd(x_1, x_2) = 1$, then x_1/x_2 is reduced *for all primes*. Letting $x_1' = x_2^4 g(P)$ and $x_2' = x_2^4 f(P)$, we observe that given any prime,

$$\varepsilon_p(P) = \mathrm{ord}_p(\gcd(x_1', x_2')),$$

and so

$$\begin{aligned}\sum_p \varepsilon_p(P)\log p &= \sum_p \min\{\mathrm{ord}_v(x_1'), \mathrm{ord}_v(x_2')\}\log p,\\ &= \log\gcd(x_1', x_2').\end{aligned}$$

Hence, if $x(2^nP) = x_{1,n}/x_{2,n}$ is reduced, we define $x_{1,n}' = x_{2,n}^4 g(P)$, $x_{2,n}' = x_{2,n}^4 f(P)$, and

$$g_n = \gcd(x_{1,n}', x_{2,n}'),$$

then taking sums we deduce that

$$\Psi_0(P) = \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log g_n.$$

This allows us construct the following algorithm for $\Psi_0(P)$ from [MS16], which implements Algorithm 2 over all primes at once.

Algorithm 3 Let $x(P) = x_1/x_2$ where $\gcd(x_1, x_2) = 1$,

1. Set $x_1' = x_2^4 g(P)$, $x_2' = x_2^4 f(P)$, $g_0 = \gcd(x_1', x_2')$ and $(x_1, x_2) = (x_1'/g_0, x_2'/g_0)$.
2. Set $D := \gcd\{\Delta(W), g_0^\infty\}$[7], where g_0^∞ means the formal product $g_0^\infty = \prod_{p|g_0} p^\infty$, and let $B := \lfloor \log D/\log 2 \rfloor$.
3. If $B \leq 1$, Return 0. Else set $m = \lfloor \log(B^5/3)/\log 4 \rfloor$.
4. For $n := 1$ to m
   (a) Compute $x_1' = x_2^4 g(P)$, $x_2' = x_2^4 f(P)$ modulo $D^{m+1} g_0$.
   (b) Set $g_n = \gcd(x_1', x_2')$, and $(x_1, x_2) = (x_1'/g_n, x_2'/g_n)$.
5. Use an algorithm to compute pairwise coprime positive integers $q_1, \ldots, q_r$ such that for all $0 \leq n \leq m$ we can write $g_n = \prod_{i=1}^r q_i^{e_{i,n}}$.
6. For $i = 1, \ldots, r$:

[7] To compute this, we can repeatedly find $\gcd(\Delta, g_0^N)$ until it stabilises.

(a) Compute

$$a = \sum_{n=0}^{m} \frac{1}{4^{n+1}} e_{i,n}. \tag{6.6}$$

(b) Let μ_i be the unique fraction in $[a, a + 1/B^4]$ with denominator bounded by B^2.

7. Return $\sum_{i=1}^{r} \mu_i \log q_i$

The algorithm for Step 5 referenced in [MS16] is given by Bernstein in [Ber05], although we wont give details here. Now, we claim that this algorithm is correct.

Proof. First note that, $\mathrm{ord}_v(g_n) = \varepsilon_v(2^n P) \leq \mathrm{ord}_v(\Delta)$, hence

$$p^{\mathrm{ord}_v(g_n)} \mid p^{\mathrm{ord}_v(\Delta)}, \quad \forall \text{ primes } p$$

and so $g_n \mid \Delta$. Now, to verify step 1, suppose that $B \leq 1$, so $D \leq 3$. If $D = 1$, then $g_0 = 1$ and $\varepsilon_p(P) = \mathrm{ord}_p(1) = 0$ for all p, so $\mu_p(P) = 0$ by Lemma 6.5, and thus $\Psi_0(P) = 0$. Otherwise $D = 2, 3$, so $g_0 = p^a, a \geq 1$ where $p = 2$ or 3. In this case $\mathrm{ord}_p(\Delta) = 1$, so W is minimal at p with Tamagawa index equal to 1. Hence $P \in E_0(\mathbb{Q}_p)$, and we have $\varepsilon_p(P) = a = 0$, which is a contradiction. Hence we must have $D = 1$ and $\Psi_0(P) = 0$.

If p is a prime such that $p \nmid g_0$, then $\varepsilon_p(P) = 0$, and so $\mu_p(P) = 0$ by Lemma 6.5. So, suppose that $p \mid g_0$. We have $\mathrm{ord}_p(\Delta) = \mathrm{ord}_p(D) \leq B$, hence B works for both bounds introduced in Lemma 6.6. Recall that in Algorithm 2 we need to compute x_1', x_2' to $(m+1)\mathrm{ord}_p(\Delta) + 1$ p-adic digits of precision to ensure the output is correct. In this case, we note that since $p^{(m+1)\mathrm{ord}_p(\Delta)+1} \mid D^{m+1} g_0$, calculating x_1', x_2' modulo $D^{m+1} g_0$ in Step 4.(a) ensures that that we have sufficient precision for *all* primes p.

Having factored into coprimes as described in Step 5, for any prime p dividing g_0, there exists a unique $i = i(p)$ such that $p \mid q_i$. Then setting $b_p = \mathrm{ord}_p(q_{i(p)})$ we deduce that,

$$\sum_{n=0}^{m} \frac{1}{4^{n+1}} \varepsilon_p(2^n P) = \sum_{n=0}^{m} \frac{1}{4^{n+1}} \mathrm{ord}_p(g_n) = \sum_{n=0}^{m} \frac{1}{4^{n+1}} b_p e_{i,n} = b_p a,$$

where a is as defined in equation (6.6). Then

$$\mu_p(P) = b_p a + \sum_{n=m+1}^{\infty} \frac{1}{4^{n+1}} \varepsilon_p(2^n P),$$

where the sum on the right is in the interval $[0, 1/B^4]$ by our choice of m and the bounds on ε_p. Now, since g_n are products of the q_i's, and $g_n \mid D$ for all n, we deduce that $b_p = \mathrm{ord}_p(q_{i(p)}) \leq \mathrm{ord}_p(D) \leq B$. Hence $\mu_{i(p)} = \mu_p(P)/b_p$ is the unique rational with denominator bounded by B^2 lying in the interval $[a, a + 1/B^4]$.
Lastly, we may put all of this together to get

$$\Psi_0(P) = \sum_p \log(p) \mu_p(P) = \sum_p \mu_{i(p)} b_p \log(p) = \sum_{i=1}^{r} \mu_i \sum_{p \mid q_i} b_p \log(p) = \sum_{i=1}^{r} \mu_i \log(q_i),$$

as required. □

A natural measure of the size of our input is in terms of $h(P) + \log \Delta$, while the output is measured in terms of t, the number of bits to we wish to compute $\hat{h}_0(P)$. We may group these into $\tau = h(P) + \log \Delta + t$ to compare the two algorithms. By throwing away the Archimedean term in [MS16, Theorem 1.1], we quote that computing $h_0(P)$ to t bits of precision using Algorithm 3 has time complexity

$$O(\log \tau \mathcal{M}[\tau] + \log \tau \mathcal{M}[\tau \log \tau])$$

where $\mathcal{M}(N)$ is the time complexity of multiplying two N-bit integers, which is $O(N\log(N)^m)$ for some constant m. Hence computing $h_0(P)$ using Algorithm 3 gives a *polynomial time* algorithm in τ. Comparing this with the task of factorising Δ, for which there is no known polynomial time algorithm, we see that Algorithm 3 is more efficient for elliptic curves with large discriminant.
In practice, a combination of methods - those with and without needing factorisation - should be used in order to compute the non-Archimedean height as efficiently as possible. For example, notice that any prime not dividing g_0 must have $\mu_v(P) = 0$, which follows from Lemma 6.5. Hence if we can factorise g_0, which may be a simpler task than factoring Δ, then Silverman's method may again be used. In a similar vein, Silverman has produced a method [Sil97] which only requires the factorisation of $\gcd(c_4, c_6)$. An efficient approach may trail factorise these terms up to some large prime P, then use Algorithm 3 if this factorisation is unsuccessful.

It is clear that Algorithm 3 is heavily reliant on computing gcd's in $\mathbb{Z}$, which is a fast computation using Euclid's algorithm. Suppose now that K is a general number field, then we immediately run into a problem since $\mathcal{O}_K$ may not be a UFD, so it is not guaranteed that gcd's even exist. Instead, we may have to consider finding greatest common divisors of ideals, or perhaps embed K into an extension L which has class number 1.[8] Even if $\mathcal{O}_K$ *is* a UFD, there is the problem of how to compute the gcd of two elements. In the case where $\mathcal{O}_K$ is a Euclidean domain, we may use Euclid's algorithm as in $\mathbb{Z}$, however if not then other techniques will need to be employed if one is to extend this algorithm more generally.

7 Local Height at Archimedean Places

We now turn to computing the Archimedean contribution $\hat{h}_\infty$ to the canonical height, which is defined in the obvious way,

$$\hat{h}_\infty(P) = \frac{1}{K:\mathbb{Q}} \sum_{v \in M_K^\infty} n_v \lambda_v(P).$$

Notice that since there are only finitely many Archimedean primes of K, we can simply calculate $\lambda_v(P)$ separately and add them together. To compute $\lambda_v(P)$, we present two methods, the first of which is a variant of a series given by Silverman in [Sil88], while the second uses the explicit formula for λ_v as is shown in [Coh93].

7.1 Simple Series method

The first method employs the definition for λ_v which we gave in equation (4.3), that is, for $P \in E(K_v)\backslash\{O\}$

$$\lambda_v(P) = \log \max\{1, |x(P)|_v\} + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_v(2^i P), \tag{7.1}$$

where we recall that $\Phi_v(P) = \frac{\max\{|f(P)|_v, |g(P)|_v\}}{\max\{1, |x(P)|_v^4\}}$. The approach taken in [Sil88] uses a similar series expansion for λ_v, which is

$$\lambda_v(P) = \log |x|_v + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} z(2^i P)$$

where $z(P) = \frac{1}{x(P)^4} g(P)$. However this only converges provided $|x(2^i P)|_v$ doesn't get arbitrarily small, so we aim to circumvent this problem by using (7.1) which converges for all P and has almost identical convergence properties. To get error estimates for the series we shall bound $\log(\Phi_v(P))$, and so seek constants c_1, c_2 such that for all $P \in E(K_v)$,

$$0 < c_1 \leq \Phi_v(P) \leq c_2,$$

which we have already shown exist by Proposition 4.1. These constants can be found computationally, which is the topic of Section 10, but we can also find bounds theoretically as follows. First, we quote the following auxiliary Lemma from [Sil88],

[8] Although, there may not be such a finite embedding - as discussed in [CF10, Ch.IX].

Lemma 7.1 Let $F(X), G(X) \in \mathbb{C}[X]$ where $\deg(F) = m, \deg(G) = n$. Then for all $x \in \mathbb{C}$,

$$\max\left\{\frac{|F(x)|}{|F|}, \frac{|G(x)|}{|G|}\right\} \geq \frac{|\mathrm{Res(F,G)}|}{2^{mn}|F|^n|G|^m} \min\left\{\frac{1}{2^m(m+1)^{n-1}}, \frac{1}{2^n(n+1)^{m-1}}\right\} \tag{7.2}$$

where $|F|$ is the maximum of the absolute values of the coefficients of F, and similarly for G.

This allows us to prove the following,

Lemma 7.2 Let E/K be an elliptic curve with Weierstrass equation W, and let v be an Archimedean place of K. Define H to be

$$H = \max\{4, |b_2|_v, 2|b_4|_v, 2|b_6|_v, |b_8|_v\},$$

then for all $P \in E(K_v) \setminus \{O\}$, we have

$$\frac{|\Delta|_v^2}{2^{26}H^9} \leq \Phi_v(P) \leq 4H \tag{7.3}$$

Proof. For the upper bound, we simply split into cases where $|x|_v \geq 1$ and $|x|_v \leq 1$. In the first case we have

$$\begin{aligned}
\Phi_v(P) &= \frac{\max\{|4x^3 + b_2x^2 + 2b_4x + b_6|_v, |x^4 - b_4x^2 - 2b_6x - b_8|_v\}}{|x|_v^4}, \\
&\leq \max\{4|x|_v^{-1} + |b_2|_v|x|_v^{-2} + 2|b_4|_v|x|_v^{-3} + |b_6|_v|x|_v^{-4}, \\
&\qquad 1 + |b_4|_v|x|_v^{-2} + 2|b_6|_v|x|_v^{-3} + |b_8|_v|x|_v^{-4}\}, \\
&\leq \max\{4 + |b_2|_v + 2|b_4|_v + |b_6|_v, 1 + |b_2|_v + 2|b_6|_v + |b_8|_v\}, \\
&\leq 4H.
\end{aligned}$$

The situation for $|x|_v \leq 1$ is almost identical,

$$\begin{aligned}
\Phi_v(P) &= \max\{|4x^3 + b_2x^2 + 2b_4x + b_6|_v, |x^4 - b_4x^2 - 2b_6x - b_8|_v\}, \\
&\leq \max\{4 + |b_2|_v + 2|b_4|_v + |b_6|_v, 1 + |b_2|_v + 2|b_6|_v + |b_8|_v\}, \\
&\leq 4H.
\end{aligned}$$

To find lower bounds, we again split into cases. First suppose that $|x|_v \geq 2\sqrt{H}$, then

$$\Phi_v(P) \geq \frac{|g(P)|_v}{|x|_v^4} = |1 - b_4x^{-2} - 2b_6x^{-3} - b_8^{-4}|_v \geq 1 - \frac{1}{|x^2|_v}|b_4 - 2b_6x^{-1} - b_8^{-2}|_v \geq 1 - \frac{1}{4H}3H = \frac{1}{4}.$$

Next, applying Lemma 7.1 to f, g, and recalling from Proposition 4.1 that $\mathrm{Res}(f, g) = \Delta^2$, we deduce that for all $P \in E(K_v)$

$$\max\{|f(P)|_v, |g(P)|_v\} \geq \frac{|\Delta|_v^2}{2^{22}H^7},$$

and so for all $|x|_v \leq 2\sqrt{H}$ we have,

$$\Phi_v(P) \geq \frac{|\Delta|_v^2}{2^{26}H^9}.$$

Lastly, observe that when $|x|_v \leq 1$, the inequality

$$\frac{|\Delta|_v^2}{2^{22}H^7} \leq \Phi_v(P) \leq 4H$$

holds, hence by dividing through by 2^4H^2 we find that

$$\frac{|\Delta|_v^2}{2^{26}H^9} \leq \frac{1}{4H} \leq \frac{1}{4}, \tag{7.4}$$

and so the inequalities in the lemma's statement hold for all $P \in E(K_v)$. □

Such bounds allow us to estimate the error in computing $\lambda_v(P)$ by truncating the series in (7.1), which is analogous to [Sil88, Theorem 4.2].

Theorem 7.3 Let $R(N)$ be the error term due to truncating the series at the Nth term, so

$$\lambda_v(P) = \log \max\{1, |x(P)|_v\} + \sum_{i=0}^{N-1} \frac{1}{4^{i+1}} \log \Phi_v(2^i P) + R(N).$$

Then

$$\frac{1}{3 \cdot 4^N} \log\left(\frac{|\Delta|_v^2}{2^{26} H^9}\right) \leq R(N) \leq \frac{1}{3 \cdot 4^N} \log(4H),$$

and so to compute $\lambda_v(P)$ to t decimal places, it is sufficient to take

$$N \geq \frac{t \log 10}{\log 4} + \frac{\log\left(\frac{1}{3}\log\left(\frac{2^{26}H^9}{|\Delta|_v^2}\right)\right)}{\log 4}.$$

Proof. First, by taking logs of equation (7.3) we deduce that,

$$\log\left(\frac{|\Delta|_v^2}{2^{26} H^9}\right) \leq \log \Phi_v(P) \leq \log(4H),$$

and so summing from N to ∞ gives the required bounds on $R(N)$. Next, if we want $\lambda_v(P)$ to t decimal places, we require $|R(N)| \leq 10^{-t}$. Observe that $|\Delta|_v^2 2^{26} H^9 < 1$, hence

$$|R(N)| \leq \frac{1}{3 \cdot 4^N} \log \max\left\{\left(\frac{2^{26}H^9}{|\Delta|_v^2}\right), 4H\right\} \overset{(7.4)}{=} \frac{1}{3 \cdot 4^N} \log\left(\frac{2^{26}H^9}{|\Delta|_v^2}\right),$$

and setting this less than or equal to 10^{-t} yields the desired inequality. □

7.2 Theta Series method

Another method for computing the local height at an real Archimedean prime is described in [Coh93, Algorithm 7.5.7], which takes a completely different approach to the series described above by using the explicit formula for $\lambda_v(P)$. The given algorithm has faster convergence, although our description only works for *real* infinite primes.

Let E/K be an elliptic curve given by Weierstrass equation W, and v a real infinite prime of K. Then there is a unique embedding $K \hookrightarrow \mathbb{R}$ associated to v, so by identifying K in $\mathbb{R}$ we view E as an elliptic curve defined over the reals. Now, in order to use the explicit formula

$$\lambda_v(P) = -2 \log |e^{-\frac{1}{2} z \eta(z;\Lambda)} \sigma(z;\Lambda)|, \tag{7.5}$$

one must first compute the periods ω_1, ω_2 of a lattice for W, as well as computing the elliptic integral z of $P \in E(\mathbb{R})$. This former task is described for curves over $\mathbb{R}$ in [Coh93, Algorithm 4.7.4], which produces periods such that

(i) ω_2 is a real positive number,

(ii) $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$, and $\mathrm{Re}\left(\frac{\omega_1}{\omega_2}\right) \in \left\{0, -\frac{1}{2}\right\}$.

Next, having found the periods we may compute the elliptic logarithm z of a point $P \in E(\mathbb{R})$ by using [Coh93, Algorithm 4.7.8], where z satisfies either

(i) z is real and $0 \leq z < \omega_2$, or

(ii) $\Delta > 0$, and $z - \frac{\omega_1}{2}$ is real, and $0 \leq z - \frac{\omega_1}{2} < \omega_2$.

The algorithms used here involved the Arithmetic-Geometric mean (AGM), and although space does not permit discussion of these algorithms, we should note that the AGM converges *quadratically*, meaning that after each iteration we know approximately twice the number of decimal points as after the previous iteration. Now, having calculated ω_1, ω_2 and z to some prescribed precision, we may finally move onto computing λ_v using the following algorithm.

Algorithm 4 : Given $a_i \in \mathbb{R}$ defining our Elliptic curve E and a point $P \in E(\mathbb{R})$, use the algorithms described above to calculate ω_1, ω_2 and $z(P)$.

1. Let $\tau = \frac{\omega_1}{\omega_2}$, $t = \frac{2\pi \mathrm{Re}(z)}{\omega_2}$, and $q = e^{2\pi i \tau}$
2. Compute the sum
$$\theta = \sum_{n=0}^{\infty} (-1)^n \sin((2n+1)t) q^{n(n+1)/2}$$
stopping when $q^{n(n+1)/2}$ is sufficiently small
3. Output:
$$\lambda_v(P) = \frac{1}{16} \log \left| \frac{\Delta}{q} \right| + \frac{1}{4} \log \left| \frac{f(P)\omega_2}{8\pi} \right| - \frac{1}{2} \log |\theta|. \tag{7.6}$$

Proof. (sketch) Define q, t and τ as in Step 1, and begin by recalling that the duplication formula is

$$\lambda_v(2P) = 4\lambda_v(P) - \log |f(P)| = 4\lambda_v(P) - \log |4x^3 + b_2 x^2 + 2b_4 x + b_6|,$$

(note: we replace $|\cdot|_v$ by $|\cdot|$ with the implicit understanding that K has been embedded into $\mathbb{R}$). Rearranging this gives

$$\lambda_v(P) = \frac{1}{4}\lambda_v(2P) + \frac{1}{4} \log |f(P)|,$$

hence comparing with equation (7.6), it suffices to show that[9]

$$\lambda_v(2P) = -2 \log |\theta| + \frac{1}{4} \log \left| \frac{\Delta}{q} \right| - 3 \log(2) - \log \pi + \log \omega_2.$$

First note that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ is an isomorphism of groups, hence $z(2P) = 2z(P)$. Now, when E is defined over $\mathbb{R}$, the value of $2z$ computed via [Coh93, Algo 7.4.8] is real, or $\Delta > 0$ and $2z - \omega_1$ is real. One can show that Δ and q have the same sign ([Sil94, p. 420]), and from the algorithm above $\mathrm{Re}(\tau) \in \{0, -1/2\}$. So if we are in the case where $\Delta > 0$, then $\mathrm{Re}(\tau) = 0$. Therefore, either $2z = \mathrm{Re}(2z)$, or $2z - \omega_1 = \mathrm{Re}(2z)$, and in both cases $\mathrm{Re}(2z)$ is a representative of $2P$ in $\mathbb{C}/\Lambda$. Dividing through by ω_2, we deduce that $\beta = 2\mathrm{Re}(z)/\omega_2$ represents $2P$ under the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$.

Recall from the end of Section 4 that the local height function is dependent on the lattice. Indeed, the lattice Λ with periods ω_i corresponds[10] to the Weierstrass equation W which use to define $E/\mathbb{C}$, however the lattice Λ_τ has a *different* Weierstrass equation W_τ. By Corollary 4.9 we have,

$$\lambda_v^{(W)}(P) = \lambda_v^{(W_\tau)}(P) + \frac{1}{6} \log \left| \frac{\Delta(W)}{\Delta(W_\tau)} \right|,$$

where the superscripts now indicate which Weierstrass the local height is defined with respect to. A simple calculation using the explicit series of g_2, g_3 in equation (5.2) implies that $\Delta(W) = \omega_2^{-12} \Delta(W_\tau)$.

[9] The idea behind this is that $2P$ is guaranteed to be on the connected component of the curve.

[10] There is a slight subtlety here, as equation (5.2) is a shortened Weierstrass equation, but W isn't required to be of this form. However, recall there's a unique substitution of the form $x = x' + r, y = y + sx' + t$ to make W shortened, and this doesn't change the discriminant, so has no affect on the local height.

Now, in [Sil94, Ch. 1, Theorem 6.4], it is shown that $\sigma(z;\Lambda_\tau)$ has the expansion

$$\sigma(\beta,\Lambda_\tau) = -\frac{1}{2\pi i} e^{\frac{1}{2}\eta(1)\beta^2} e^{-i\pi\beta}(1-u)\prod_{n\geq 1}\frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2},$$

and using Legendre's relation we have $\eta(1;\Lambda_\tau)\beta - \eta(\beta;\Lambda_\tau) = 2\pi i a$, where $a, b \in \mathbb{R}$ are the unique reals such that $\beta = a\tau + b$. Substituting this into the explicit formula for the lattice Λ_τ (7.5) gives

$$\begin{aligned}\lambda_v^{(W_\tau)}(2P) &= -2\log\left|\frac{1}{2\pi}\exp\left(\frac{1}{2}\eta(1)\beta^2 - \frac{1}{2}\eta(\beta)\beta\right)e^{-i\pi\beta}(1-u)\prod_{n\geq 1}\frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2}\right|,\\ &= -2\log\left|\frac{1}{2\pi}(1-u)\prod_{n\geq 1}\frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2}\right|,\end{aligned} \tag{7.7}$$

where $u = \exp(2i\pi\beta) = \exp(2it)$. Next, introduce the theta series;

$$\theta(u,q) = \frac{i}{2q^{\frac{1}{8}}}\sum_{n\in\mathbb{Z}}(-1)^n u^{(2n+1)/2} q^{n(n+1)/2} = \sum_{n=0}^{\infty}(-1)^n \sin((2n+1)t) q^{n(n+1)/2},$$

which, by comparing the definitions[11] of θ_1 in [MM97, p.215,315] is equal to

$$\theta(u,q) = \frac{iC}{2} e^{-\pi i\beta}(1-u)\prod_{n\geq 1}(1-q^n u)(1-q^n u^{-1}),$$

with $C = \prod_{n\geq 1}(1-q^n)$. Comparing this with equation (7.7), we get

$$\lambda_v^{(W_\tau)}(2P) = -2\log\left|\frac{C^{-3}}{\pi}\theta\right|.$$

The final step is noting that $\Delta(W) = \omega_2^{12}\Delta(W_\tau) = \omega_2^{-12}(2\pi)^{12} q C^{24}$ (see [Sil94, p.468]), and so

$$\begin{aligned}\lambda_v^{(W_\tau)}(2P) &= -2\log\left|\frac{C^{-3}}{\pi}\theta\right| = -2\log|\theta| + \frac{6}{24}\log\left|\frac{\Delta\omega_2^{12}}{q(2\pi)^{12}}\right| + 2\log|\pi|,\\ &= -2\log|\theta| + \frac{1}{4}\log\left|\frac{\Delta}{q}\right| - \log\pi - 3\log 2 + 3\log\omega_2.\end{aligned}$$

Finally, to obtain $\lambda_v = \lambda_v^{(W)}$ from this we must subtract off $2\log\omega_2$, giving

$$\lambda_v(2P) = \lambda_v(2P) = -2\log|\theta| + \frac{1}{4}\log\left|\frac{\Delta}{q}\right| - \log\pi - 3\log 2 + \log\omega_2,$$

as required. □

It is natural to ask how many terms of the theta series we must compute to get $\lambda_v(P)$ to some desired accuracy. Indeed, suppose θ_N is the sum truncated at the Nth point and set R_N to be the remainder. To get a bound on $|R_N|$, consider

$$|R_N| = \left|\sum_{n\geq N+1}(-1)^n \sin((2n+1)t) q^{(n+1/2)^2/2}\right| \leq \sum_{n\geq N+1} q^{n^2/2} \leq \sum_{n\geq (N+1)^2} q^{n/2} \leq \frac{q^{(N+1)^2/2}}{1-q^{1/2}}$$

which is $O(q^{N^2/2})$. Then we wish to calculate

$$\log|\theta| = \log|\theta_N + R_N| = \log|\theta_N| + O(\frac{R_N}{|\theta_N|}),$$

[11] We've changed the normalisations to be more in line to Cohen's series.

so if we want t decimal places of accuracy, it suffices to take

$$N \geq \left(\frac{-2}{\log(q)} \left(\log \left(\frac{C}{|\theta_N|} \right) + t \log 10 \right) \right)^{1/2},$$

where C is some real constant. Compared to the previous series method, we have an improvement, since N grows like $t^{1/2}$ here, as opposed to growing like t in Theorem 7.3. However we note that in our (rather crude) analysis here, the lower bound for N depends on $|\theta_N|$, so if the θ-series converges to a small value we may have problem.

This method may be modified for finding $\lambda_v(P)$ for complex embeddings, although the computations of the periods and the elliptic integral $z(P)$ would involve the *complex* AGM, which is more complicated than in the real case. We should briefly note that there is also a method of computing Archimedean local heights due to Bost and Mestre. The method is faster than the theta series algorithm and empirical evidence suggests it is correct, although this hasn't yet been proven. Indeed, this algorithm has already been implemented in packages such as PARI/GP.[12]

8 Examples

We now present numerous examples of calculation of the canonical height, hoping to illustrate situations where each of the techniques discussed are useful. Unless otherwise stated, I have used the computer algebra package Sage is used to implement each algorithms discussed, as well as Bernstein's Algorithm from [Ber05]. Data on elliptic curves is obtained from [LMF24].
Example 1: Consider the following elliptic curve E over $\mathbb{Q}$;

$$W : y^2 = x^3 - 4x + 1.$$

One can show that $E(\mathbb{Q})$ has rank 2, and the discriminant of W is $\Delta = 3664$. By inspection, we find small integral points

$$P = (0, 1), \qquad Q = (2, 1),$$

and suppose we want to test the linear independence of these points. We shall therefore need to calculate the values $\langle P, P \rangle, \langle P, Q \rangle$ and $\langle Q, Q \rangle$, and so must compute $\hat{h}(P)$, $\hat{h}(Q)$ and $\hat{h}(P + Q)$, where $P + Q = (-2, -1)$. We illustrate this procedure for the point P.

Firstly, since the discriminant is small, we use Silverman's method to compute the non-Archimedean contribution. Note that $x(P) = 0$ implies that for all primes p, the value of $\log \max\{1, |x|_p\}$ is 0. Now, the discriminant is $\Delta = 3664 = 2^4 \cdot 229$, hence at $p = 229$ the curve has Tamagawa index 1, and the contribution is 0. The only non-zero contribution to the non-Archimedean height thus comes from $p = 2$, and we follow Algorithm 1, noting that W is in fact minimal at $p = 2$. Consider

$$3x^2 + 2a_2x + a_4 - a_1y = -4, \qquad 2y + a_1x + a_3 = 2,$$

hence P reduces to the singular point of $\tilde{E}$. Next, we have $\mathrm{ord}_2(c_4) = \mathrm{ord}_2(192) > 0$, so the curve has additive reduction modulo 2, and we move to Step 3 in Algorithm 1. We find that $\psi_2(P) = 2$, and $\psi_3(P) = -16$

$$\mathrm{ord}_2(\psi_3(P)) = 4 \geq 3 = 3\mathrm{ord}_2(\psi_2(P)),$$

which means that the curve has reduction type IV or IV*, and

$$\lambda_2(P) = \frac{2}{3} \log |\psi_2(P)|_2 = -\frac{2}{3} \log 2.$$

Next, we calculate the Archimedean local height of P via the Cohen algorithm above, and add this to the non-Archimedean contribution to the local height. The algorithms from [Coh93] were also implemented in Sage, and returned the local Archimedean height to be

$$\lambda_\infty(P) = 0.73483932240742...$$

[12] See https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.5.5/users.pdf page.120

which, when added to the non-Archimedean contribution implies that the canonical height is,

$$\hat{h}(P) = 0.27274120203413...$$

Repeating this process for Q, $P+Q$, we compute that

$$\det\begin{pmatrix}\langle P,P\rangle & \langle P,Q\rangle \\ \langle Q,P\rangle & \langle Q,Q\rangle\end{pmatrix} = \det\begin{pmatrix}0.54548240 & -0.15101889 \\ -0.15101889 & 1.0425258\end{pmatrix} = 0.5458727966...$$

and can therefore deduce that P, Q are linearly independent points in $E(\mathbb{Q})$.
Example 2: In this example we consider elliptic curves of large discriminant, which render the Silverman approach far less efficient than that of Muller and Stoll. Consider the following family of elliptic curves $E_a/\mathbb{Q}$, which are similar to those presented in [MS16],

$$W_a : y^2 = x^3 - ax^2 + ax = x(x^2 - ax + a),$$

for some $a \in \mathbb{Z}$. Notice that $P = (1,1)$ lies on $E_a(\mathbb{Q})$ for any a. The discriminant of W is $\Delta = -16a^3(a-4)$, so we shall choose a to be a large, difficult to factorise number. For example, taking a to be
800677605005355812799605890944532804046347530997236523888896294024225650229425428023715645343727544153715772312295299085992432260832024995516544775935872779196210796134432440068091194268074752607216 41
which has 200 digits, our program implementing Algorithm 3 in Sage took 0.00250793 seconds to compute $\hat{h}_0(P)$. When we attempt to compute the non-Archimedean contribution to the height of $P = (1,1)$ using Sage's inbuilt *height* function, which factorises the discriminant and uses Algorithm 1 to obtain the non-Archimedean contribution, the process did not terminate in over an hour.

Example 3: Lastly we consider a curve over $K \neq \mathbb{Q}$, which has a complex primes. Let $K = \mathbb{Q}(i)$ and define E/K by the Weierstrass equation

$$W : y^2 = x^3 - x^2 + 2ix - 2i.$$

Let's suppose we'd like to compute the height of $P = (1+i, 2i) \in E(\mathbb{Q}(i))$. Factoring the discriminant into primes gives $\Delta = 512 + 384i = (1+i)^{14} \cdot (1+2i)^2$, and we find that W is minimal at both of these primes. Applying Silverman's algorithm then gives

$$\hat{h}_0(P) = -\frac{3}{4}\log(2).$$

For the Archimedean contribution, we note that K has one infinite prime, which is complex, and we shall use the simple series method to compute. To calculate the local height to 20 decimal place, it suffices by Theorem 7.3 to take $N \geq \frac{20\log 10}{\log 4} + \frac{\log\left(\log(2^{26}H^9/|\Delta|^2/3\right)}{\log 4} \approx 33.915$. So, for $N = 34$, the local height was computed to be

$$\lambda_\infty(P) = 0.80808456473358570450...$$

and so the canonical height is

$$\hat{h}(P) = 0.28822417931362672243...$$

Part III
Bounding the Difference Between Naive and Canonical Height

In this part of the essay we turn to computing bounds for the difference between the naive height and the canonical height of points on $E(K)$. To do so, we once again decompose into local components as follows

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

Our exposition mainly follows [CPS06] and [Bru13], the former of which uses the series definition of Ψ_v as given in equation (8.1), while the latter uses the explicit formulas for the local height at Archimedean places. Let E/K be an elliptic curve with coefficients in $\mathcal{O}_K$, $v \in M_K$ a place on K, and recall that Ψ_v is a bounded function on $E(K_v)$ defined by

$$\Psi_v(P) = \log \max\{1, |x(P)|_v\} - \lambda_v(P) = -\sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_v(2^i P), \tag{8.1}$$

with $\Phi_v(P)$ defined as usual. We begin by quoting a result from [Bru13, Theorem 2.1], which says that if we can find the infimum and supremum of Ψ_v for each v over $E(K_v)$, then we get *optimal* bounds for the height differences when working over $\overline{\mathbb{Q}}$.

Theorem 8.1 Let E/K be an elliptic curve given by Weierstrass equation W with coefficients in $\mathcal{O}_K$, we have

$$\inf_{P \in E(\overline{\mathbb{Q}})} (h(P) - \hat{h}(P)) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \inf_{P \in E(K_v)} (\Psi_v(P))$$

$$\sup_{P \in E(\overline{\mathbb{Q}})} (h(P) - \hat{h}(P)) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \sup_{P \in E(K_v)} (\Psi_v(P)).$$

So computing the extrema locally will give optimal bounds for the height difference over $E(\overline{\mathbb{Q}})$. Although these bounds may not be optimal over $E(K)$, it certainly motivates seeking the extrema of the local differences.

9 Bounds for Non-Archimedean Local Heights

The non-Archimedean case is far simpler than the Archimedean one, and we have in fact already found the bounds in Proposition 6.4, which we shall restate here,

Proposition 9.1 Let E/K be an elliptic curve, and let v be in M_K^0. Suppose E is given by a v-integral Weierstrass equation W, which is not necessarily minimal. We have

$$\inf_{P \in E(K_v)} \Psi_v(P) = 0,$$

which is attained for some $P \in E_0(K_v)$, and

$$\sup_{P \in E(K_v)} \Psi_v(P) = \left(\alpha_v + \frac{1}{6} \mathrm{ord}_v \left(\frac{\Delta}{\Delta^{\min}} \right) \right) \frac{\log \# k_v}{n_v},$$

where α_v is as given in Table 3 , and $\Delta^{\min}$ is the discriminant of a minimal Weierstrass equation for E at v.

Kodaira Type	Tamagawa index c_v	α_v
Any	1	0
I_m, $m \geq 2$	m	$m/4$
I_m, $m \geq 2$ even	2	$m/4$
III	2	1/2
IV	3	2/3
I_0^*,	4 or 2	1
I_m^*	4	1
I_m^*	2	$(m+4)/4$
IV^*	3	4/3
III^*	2	3/2

Table 3: Bounds α_v for $\mu_v(P)$, where the elliptic curve has minimal Weierstrass equation.

So we've found sharp bounds for $\Psi_v(P)$ over $E(K_v)$, and note that if the map $E(K) \to E(K_v)/E_0(K_v)$ is surjective, then they will also be optimal bounds of $\Psi_v(P)$ for $P \in E(K)$.

Thus to find the local bounds at a given non-Archimedean place, we simply apply Tate's algorithm to compute the Kodaira symbol, then read off the corresponding values. However, to efficiently do this over *all* non-Archimedean values, we will require the factorisation of the discriminant (Δ).

10 Bounds for Archimedean Local Heights

Now let $v \in M_K^\infty$ be an Archimedean place of K, and as usual let E/K an elliptic curve defined by a Weierstrass equation W.

10.1 CPS method

One method of bounding Ψ_v is to use the series

$$\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_v(2^i P),$$

since if one can bound $\log \Phi_v(P)$ on $E(K_v)$, then it is simple to show that for all $P \in E(K_v)$,

$$\frac{1}{3} \inf_{Q \in E(K_v)} \left(-\log \Phi_v(Q)\right) \leq \Psi_v(P) \leq \frac{1}{3} \sup_{Q \in E(K_v)} \left(-\log \Phi_v(Q)\right). \tag{10.1}$$

Now, in Proposition 4.1 we noted that $\Phi_v(P)$ is a continuous, bounded function with infimum greater than zero, hence we may define

$$\epsilon_v = \inf_{P \in E(K_v)} \{\Phi_v(P)\}^{-1}, \qquad \delta_v = \sup_{P \in E(K_v)} \{\Phi_v(P)\}^{-1},$$

which neatens up equation (10.1) to read,

$$\frac{\log \delta_v}{3} \leq \Psi_v(P) \leq \frac{\log \epsilon_v}{3}.$$

So, the goal of this section is to compute the values δ_v and ϵ_v, which we can separate into the cases of real and complex places.

10.1.1 Real Case

Suppose that v is a real place of K with $\sigma : K \hookrightarrow \mathbb{R}$ the corresponding embedding. We shall use this to identify $K \hookrightarrow \mathbb{R}$. Recall that f, g are the polynomials

$$f(x) = 4x^3 + b_2 x^2 + 2b_4 x + b_6,$$
$$g(x) = x^4 - b_4 x^2 - 2b_6 x - b_8,$$

and to ease notation, define

$$F(x') = x'^4 f\left(\frac{1}{x'}\right), \qquad G(x') = x'^4 g\left(\frac{1}{x'}\right).$$

A point $(x, y) \in \mathbb{R}^2$ is on $E(\mathbb{R})$ if and only if $f(x) = (2y + a_1 x + a_3)^2$, and so for all $x(P)$ where $P \in E(\mathbb{R}) \setminus \{O\}$ we must have $f(x(P)) \geq 0$. This motivates defining the sets D, D',

$$D = \{x \in [-1, 1] : f(x) \geq 0\}, \qquad D' = \{x' \in [-1, 1] : F(x') \geq 0\}$$

so that

$$\{x(P) \in \mathbb{R} : P \in E(\mathbb{R})\} = D \cup \left\{\frac{1}{x'} : x' \in D'\right\}.$$

The we have

$$\Phi_v(P) = \begin{cases} \max\{|f(x(P))|, |g(x(P))|\} & \text{if } x(P) \in D \\ \max\{|F(x'(P))|, |G(x'(P))|\} & \text{if } x'(P) = 1/x(P) \in D', \end{cases}$$

which is useful because we've reduced our task to finding the extrema over finite closed intervals. Thus, defining the values

$$e = \inf_{x\in D} \max\{|f(x)|, |g(x)|\}, \quad e' = \inf_{x'\in D'} \max\{|F(x')|, |G(x')|\}$$
$$d = \sup_{x\in D} \max\{|f(x)|, |g(x)|\}, \quad d' = \sup_{x'\in D'} \max\{|F(x')|, |G(x')|\}.$$

implies that

$$\inf_{P\in E(\mathbb{R})} \Phi_v(x) = \min\{e, e'\}, \qquad \sup_{P\in E(\mathbb{R})} \Phi_v(x) = \max\{d, d'\},$$

which gives rise to the following algorithm.

Algorithm 5 Given W a Weierstrass equation with coefficients $a_i \in \mathbb{R}$, we compute e, e', d, d' as follows:

1. Compute the set T consisting of ± 1 and the zeros of the polynomials $f, f', g, g', f-g, f+g$ that lie in the interval $[-1, 1]$. Similarly compute the set T' containing ± 1 and the zeros of the polynomials $F, F', G, G', F-G, F+G$ that lie in the interval $[-1, 1]$.
2. Set $e = \min_{x\in T} \max\{|f(x)|, |g(x)|\}$, $e' = \min_{x'\in T'} \max\{|F(x')|, |G(x')|\}$, $d = \max_{x\in T} \max\{|f(x)|, |g(x)|\}$, $d' = \max_{x'\in T'} \max\{|F(x')|, |G(x')|\}$.

The validity of this follows as one can show that the extrema of $\max_{x\in D}\{|f(x)|, |g(x)|\}$ are attained at some $x \in T$, and similarly for the case of F, G and T'.

10.1.2 Complex Case

The complex case is slightly more difficult, and [CPS06] gives two approaches, the first of which is more technical and relies on solving simultaneous equations of polynomials in two variables. We shall present the second method, which is more computational and uses repeated quadrisection of domains in $\mathbb{C}$ to compute ϵ_v and δ_v to arbitrary accuracy.

Let v be a complex Archimedean place, so $K_v = \mathbb{C}$ and again we may identify K in $\mathbb{C}$ by choosing one of the complex embeddings associated to v. Let f, g, F, G be as previously defined, and let D be the closed unit disc $\{z \in \mathbb{C} : |z| \leq 1\}$. Then we have

$$\Phi_v(P) = \begin{cases} \max\{|f(x(P))|, |g(x(P))|\} & \text{if } x \in D \\ \max\{|F(x'(P))|, |G(x'(P))|\} & \text{if } x'(P) = 1/x(P) \in D \end{cases}$$

Thus we are interested in computing the extrema over $z \in D$ of

$$\max\{|P(z)|, |Q(z)|\}$$

where $P, Q \in \mathbb{C}[Z]$ are coprime polynomials. Hence define functions α, β as follows,

$$\alpha(P, Q) = \inf_{z\in D} \max\{|P(z)|, |Q(z)|\}$$
$$\beta(P, Q) = \sup_{z\in D} \max\{|P(z)|, |Q(z)|\}.$$

from which we have

$$\inf_{P\in E(\mathbb{C})} \Phi_v(x) = \min\{\alpha(f, g), \alpha(F, G)\}, \qquad \sup_{P\in E(\mathbb{C})} \Phi_v(x) = \max\{\beta(f, g), \beta(F, G)\}.$$

Let μ be the desired accuracy to which we want to compute $\log \epsilon_v$ and $\log \delta_v$, so we want to find $\alpha^*(P, Q)$ and $\beta^*(P, Q)$ such that

$$\begin{aligned} \alpha^*(P, Q)e^{-\mu} \leq &\alpha(P, Q) \leq \alpha^*(P, Q), \\ \beta^*(P, Q) \leq &\beta(P, Q) \leq \beta^*(P, Q)e^{\mu}, \end{aligned}$$

To ease notation, define $h(z) = \max\{|P(z)|, |Q(z)|\}$, and as in [CPS06] define

$$\mathcal{E}(u,\eta) = \max\left\{\sum_{n=1}^{\deg P} \frac{\eta^n}{n!}|P^{(n)}(u)|, \sum_{n=1}^{\deg Q} \frac{\eta^n}{n!}|Q^{(n)}(u)|\right\},$$

for $\eta \in \mathbb{R}$. Taylor's theorem says that for $t \in \mathbb{C}$ we have

$$P(z) = P(u+t) = P(u) + \sum_{n=1}^{\deg P} \frac{t^n}{n!}P^{(n)}(u),$$
$$Q(z) = Q(u+t) = Q(u) + \sum_{n=1}^{\deg Q} \frac{t^n}{n!}Q^{(n)}(u)|,$$

and so by taking maxima we deduce that for all $t \leq \eta$ and $z = u + t$

$$h(u) - \mathcal{E}(u,\eta) \leq h(z) \leq h(u) + \mathcal{E}(u,\eta). \tag{10.2}$$

In particular the following lemma is immediate,

Lemma 10.1 If $S \subset \mathbb{C}$ is a square with side length r, then the inequality (10.2) hold for all $z \in S$, where

(i) $u \in \mathbb{C}$ is the centre of S and $\eta = r/\sqrt{2}$, or

(ii) $u \in \mathbb{C}$ is a corner of S and $\eta = r\sqrt{2}$,

This lemma allows us to construct recursive algorithms for computing α^* and β^* to specified accuracy, by repeatedly quadrisecting squares as follows. We give both algorithms below, noting that there is a slight improvement for computing β^* case, since one can show using the maximum modulus theorem that $\beta(P,Q)$ is attained on the boundary ∂D of D.

Algorithm 6 (S, t, μ, P, Q)
Inputs: $S = [a, a+r] \times [b, b+r]$ a square, t the current estimate of α^* or β^*, μ the desired accuracy, and P, Q coprime complex polynomials.

1. If
$$\begin{cases} S \cap D = \emptyset & \text{when computing } \alpha^* \\ S \cap \partial D = \emptyset & \text{when computing } \beta^* \end{cases}$$
then Return t,

2. If the centre $(a + r/2, b + r/2)$ of S is in D, then set $u = (a + r/2, b + r/2)$ and $\eta = r/\sqrt{2}$, else let u be a corner of S in D and $\eta = r\sqrt{2}$.

3. If
$$\begin{cases} h(u) - \mathcal{E}(u,\eta) > te^{-\mu} & \text{when computing } \alpha^* \\ h(u) + \mathcal{E}(u,\eta) < te^{\mu} & \text{when computing } \beta^* \end{cases}$$
then Return t;

4. Set $t = \begin{cases} \min\{t, h(u)\} & \text{when computing } \alpha^* \\ \max\{t, h(u)\} & \text{when computing } \beta^* \end{cases}$,

5. Divide S into quarters $S_1, \ldots, S_4$. For i =1 to 4:
$$\text{Set } t = \text{Algorithm6}(S_i, t, \mu, P, Q).$$

6. Return t.

In order to find α^* or β^*, we apply Algorithm 6 to the square $[-1,1]^2$, with some starting guess for t. This can be obtained simply by calculating $h(z)$ for some initial sample of points in D, and taking the min/max as necessary. The proof of the validity of the algorithm computing α^* is given in [CPS06], for variety we give a brief proof that the β^* algorithm works, which it is near identical.

Proposition 10.2 Algorithm described terminates, and returns $\beta^*(P,Q)$ such that $\beta^* \leq \beta(P,Q) \leq \beta^* e^{\mu}$, for some $\mu > 0$ given.

Proof. Recall that β is the supremum of $h(z)$ over the unit disc D. By the maximum modulus theorem, this supremum must lie on the boundary ∂D of the disc, as the supremum of h must also be a supremum of $|P|$ or $|Q|$ over D. The initial estimate for β^* is the maximum of $h(u)$ taken over a sample of $u \in D$, and the value of only ever changes in Step 4 where we replace it by $\max\{\beta^*, h(u)\}$, with $u \in D$. Therefore, throughout the algorithm we have $\beta^* \leq \beta(P,Q)$.
If we leave a square without quadrisecting it, either $S \cap \partial D = \emptyset$, or

$$h(u) + \mathcal{E}(u,\eta) < \beta^* e^{\mu},$$

and by Lemma 10.1, we have $h(z) < h(u) + \mathcal{E}(u,\eta)$ for all $z \in S$. The algorithm terminates if we've covered ∂D with squares such that this inequality holds, so $h(z) \leq \beta^* e^{\mu}$ for all $z \in \partial D$. Taking the supremum then implies that $\beta(P,Q) \leq \beta^* e^{\mu}$.
So it remains to show that the algorithm terminates, which can be done by contradiction. If the algorithm doesn't terminate, then there is an infinite sequence of nested squares S_i of side length $1/2^i$ and centre $u_i \in D$. Since they're nested, (u_i) must converge, and moreover we have a sequence of reals η_i converging to 0, with

$$h(u_i) + \mathcal{E}(u_i,\eta_i) \geq \beta_i^* e^{\mu},$$

where

$$\beta_i^* = \max\{h(u_j) : j = 1,\dots,i\}.$$

The formula for $\mathcal{E}$ implies that as $i \to \infty$, we have $\mathcal{E}(u_i,\eta_i) \to 0$, hence taking the limit of the inequality, and noting that β_i^* is convergent (as is increasing and bounded above), we find that

$$\lim_{i\to\infty} \beta_i^* e^{\mu} \leq \lim_{i\to\infty} h(u_i) \leq \lim_{i\to\infty} \beta_i^*,$$

which is a contradiction.

□

One may notice that the definitions of local height seem to depend on the duplication map, as opposed to multiplication by some arbitrary $m \in \mathbb{Z}$. For example, in Theorem 4.8, we have λ_v is the unique function satisfying properties (i),(ii), and the duplication formula

$$\lambda_v(2P) = 4\lambda_v(P) - \log|f(P)|.$$

It turns out that we may replace this condition by any $m \in \mathbb{Z}$, replacing $f(P)$ by some suitable polynomial $f_m(P)$, as discussed in Sections 4,5 of [Uch08]. Then we can replace $\Phi_v(P)$ with an analogous function $\Phi_{m,v}(P)$, and by uniqueness of λ_v we deduce that

$$\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{m^{i+1}} \log \Phi_{m,v}(m^i P).$$

Generalising the results of the previous section, one can bound $\Phi_{m,v}$ by $\epsilon_{m,v}^{-1}, \delta_{m,v}^{-1}$, which gives

$$\frac{\log \delta_{m,v}}{m^2-1} \leq \Psi_v(P) \leq \frac{\log \epsilon_{m,v}}{m^2-1}.$$

The use of this generalisation is that as $m \to \infty$, these bounds become arbitrarily close to the optimal bounds over $E(K_v)$, as given in [Uch08, Cor. 21], and for any fixed m we can calculate $\epsilon_{m,v}, \delta_{m,v}$ using the same methods as discussed above.

10.2 Bounds over a Fundamental Domain

In a similar vein to section 7, we may ask whether the explicit formula and the complex theory of elliptic curves can be used to calculate better bounds for Ψ_v. Given an elliptic curve E over $\mathbb{C}$ with Weierstrass equation W, recall that there is an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some lattice Λ, and

$$\lambda_v(z) = -2\log|e^{-\frac{1}{2}z\eta(z;\Lambda)}\sigma(z;\Lambda)|,$$

where z is the image of P in $\mathbb{C}/\Lambda$. We can then subtract this from $\log\max\{1,|x(P)|\}$ to get

$$\Psi_v(z) = \max\{1,|\wp(z;\Lambda) - b_2/12|\} - -2\log|e^{-\frac{1}{2}z\eta(z;\Lambda)}\sigma(z;\Lambda)|,$$

noting that $x(P) = \wp(z;\Lambda) - b_2/12$. Importantly, since this is periodic in Λ, we only have to search over a fundamental domain of Λ to find the extrema. If we can find a result similar to (10.2) in the previous section, then we may again use repeated quadrisection to of this domain to compute the extrema of Ψ_v, as opposed to just Φ_v, over $E(\mathbb{C})$.

This is the method explored in [Bru13], and it allows us to find *optimal* bounds for Ψ_v over $E(\mathbb{C})$ to arbitrary precision. The proofs given rely heavily on working with complex differentials, so we shall simply state the main results and give an Algorithm which can be used to implement them.

Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass equation W, and let $\Lambda = \omega_1\mathbb{Z}+\omega_2\mathbb{Z} \subset \mathbb{C}$ be a corresponding lattice. Consider a parallelogram $R(z_0,z_1,z_2) = \left\{z_0 + s_1z_1 + s_2z_2 \in \mathbb{C} : s_i \in \left[-\frac{1}{2},\frac{1}{2}\right]\right\}$, where z_1, z_2 are linearly independent over $\mathbb{R}$, and observe that for all $z \in R(z_0,z_1,z_2)$ we have

$$|z - z_0| \leq d(z_1,z_2), \qquad \text{where } d(z_1,z_2) = \frac{1}{2}\max\{|z_1+z_2|,|z_1-z_2|\}.$$

Bruin's paper culminates in showing that there exists a constant M depending only on Λ, such that for all $z \in R(z_0,z_1,z_2)$,

$$|\Psi_v(z) - \Psi_v(z_0)| \leq 2d(z_1,z_2)M.$$

We may view this as an analogous result to Lemma 10.1, and can therefore construct a recursive algorithm to calculate the extrema of $\Psi_v(z)$ over $z \in \mathbb{C}/\Lambda$ in a similar way. Below we present an algorithm to find the supremum of $\Psi_v(z)$,

Algorithm 7 (W, R, Ψ_v^*, μ)
Inputs: W the Weierstrass equation defining E, $R = R(z_0,z_1,z_2)$ the parallelogram we're considering, Ψ_v^* our current estimate for $\sup\Psi_v$, and μ the desired accuracy.

1. Compute $\Psi_v(z_0)$. If $\Psi_v(z_0) + 2Md(z_1,z_2) < \Psi_v^* + \mu$, Return Ψ_v^*.
2. Let $\Psi_v^* = \max\{\Psi_v^*, \Psi_v(z_0)\}$
3. Divide R into quarters $R_1,\ldots,R_4$, with centres $z_0 \pm \frac{1}{4}(z_2 \pm z_1)$ then for $i = 1$ to 4:

   $$\text{Set } \Psi_v^* = \text{Algorithm7}(W, R_i, \Psi_v^*, \mu)$$

4. Return Ψ_v^*.

Applying this algorithm to a fundamental domain of Λ will return $\sup_{P\in E(\mathbb{C})}\Psi_v(P)$, which can be proven in an identical way to Proposition 10.2. To get an algorithm computing $\inf\Psi_v(P)$, we simply replace the inequality in Step 1 by $\Psi_v(z_0) - 2Md(z_1,z_2) > \Psi_v^* - \mu$, and change max to min in step 2.
Notice that each time the function is called the value $\Psi_v(z_0)$ must be computed, which is essentially the entire discussion of Section 7. As the value z_0 and the periods ω_1,ω_2 are already known, it makes sense to use the explicit formula to find λ_v, then subtract this from $\log\max\{1,|x|\} = \log\max\{1,|\wp_\Lambda(z) - b_2/12|\}$. Computing λ_v can be done using Theta series in a similar way to Section 7.2, although we should note that here we aren't assuming the curve to be defined over $\mathbb{R}$.

To actually define M, we require some auxiliary definitions as follows. Let ω_1, ω_2 be the periods of Λ, and let

$$C_\Lambda = \frac{\eta(\omega_1;\Lambda)\bar{\omega}_2 - \eta(\omega_2;\Lambda)\bar{\omega}_1}{2i\text{vol}(\Lambda)}, \qquad D_\Lambda = \frac{\pi}{\text{vol}(\Lambda)},$$

where $\text{vol}(\Lambda)$ is the volume of a fundamental domain of Λ. Then let $Z(z;\Lambda)$ be

$$Z_\Lambda(z) = \zeta_\Lambda(z) - C_\Lambda z - D_\Lambda \bar{z}.$$

The paper shows that there is a continuous function W_Λ defined on $\mathbb{C}/\Lambda \setminus S$, where $S = \{z \in \mathbb{C}/\Lambda : |\wp_\Lambda(z) - b_2/12| = 1\}$, such that

$$d\Psi_v(z) = W(z)dz + \overline{W(z)}d\bar{z}.$$

Thus bounding $|W_\Lambda(z)|$ will give bounds for the difference $\Psi_v(z_0) - \Psi_v(z_1)$ by integrating over a path from z_0 to z_1. This is given by [Bru13, Corollary 4.3], which says that for any $p \in S$, we have for all $z \in \mathbb{C}/\Lambda \setminus S$,

$$|W_\Lambda(z)| \leq M = \max\left\{|Z_\Lambda(p) + M_1 J|, \left|\frac{1}{2}(Z_\Lambda(p-t_1) + Z_\Lambda(p-t_2)) + M_2 J\right|\right\}$$

where $t_i \in \mathbb{C}/\Lambda$ are the roots of the equation $\wp_\Lambda(z) = b_2/12$, and M_1, M_2, J are the constants defined as follows;

$$\begin{aligned} M_1 &= |C_\Lambda + \frac{b_2}{12}| + |D_\Lambda| + 1 \\ M_2 &= |C_\Lambda + \frac{b_2}{12}| + |D_\Lambda| + \frac{|b_4|}{2} + \frac{|b_6|}{2} \\ J &= \int_0^{2\pi} \frac{d\theta}{|4\exp(3i\theta) + b_2\exp(2i\theta) + 2b_4\exp(i\theta) + b_6|}. \end{aligned}$$

As mentioned above, every time Algorithm 7 is called we must compute $\Psi_v(z_0)$, which means it is often slower than the algorithms of Section 10.1. However, it does return arbitrarily accurate optimal bounds for the local difference over $E(\mathbb{C})$, so is useful in cases where we require even sharper bounds than those produced in Algorithm 6. However, for the case where v is a real prime, the extrema of $\Psi_v(P)$ over $E(\mathbb{R})$ may be different to those taken over $E(\mathbb{C})$, hence it is possible that the bounds computed via Algorithm 5 are better than those from Bruin's method.

11 Examples

The programming for Algorithms 5,6 was again done in Sage, while Algorithm 7 is implemented in PARI by Bruin at https://www.math.leidenuniv.nl/ pbruin/hdiff.gp.
Example 1: Here we shall extend *Example 1* from Section 8 by calculating the height difference bounds, which can subsequently be used to calculate whether the points P, Q are in fact a basis of $E(\mathbb{Q})$. Recall that $E/\mathbb{Q}$ is a rank 2 curve defined by Weierstrass equation

$$W : y^2 = x^3 - 4x + 1,$$

and we have shown that $P = (0,1), Q = (2,1)$ are linearly independent points. In order to test whether these points are generators, we must compute bounds for $h - \hat{h}$ over $E(\mathbb{Q})$. Since $\mathbb{Q}$ only has one Archimedean place, which is real, we begin by implementing the algorithm of Section 10.1.1, which is again done in Sage. Using this method, the lower and upper bounds for Ψ_∞ were calculated to be

$$-1.16550252... \leq \Psi_\infty \leq 0.000000...$$

As for the non-Archimedean case, recall that $\Delta = 2^4 \cdot 229$, hence the only contribution will come from $p = 2$, where the Kodaira symbol was found to be IV. Hence reading from Table 3 we have $\alpha_2 = 2/3$, so

$$0 \leq \Psi_2 \leq 2/3\log(2).$$

Moreover, having shown that $\lambda_2(P) = -2\log(2)/3$, we know that these bounds are sharp. Combining these two results, the global bounds are

$$-1.16550252... \leq h - \hat{h} \leq 0.46209812.$$

Example 2: Lastly, we consider the number field $K = \mathbb{Q}(\zeta_5)$, which has two complex embeddings ∞_1, ∞_2, and is a PID. Let E/K be the elliptic curve defined by

$$W : y^2 = x^3 - \zeta_5 x + 1.$$

The discriminant of W is $\Delta = 64\zeta_5^3 - 432$, and this has factorisation $\Delta = -\zeta_5^2 \cdot 2^4 \cdot (\zeta_5^3 - \zeta_5 + 1) \cdot (\zeta_5^3 - 13\zeta_5^2 - 6\zeta_5 + 6)$. Noting that ζ_5 is just a unit, the only non-Archimedean contribution comes from the prime (2), where E has Kodaira symbol III. Hence we have

$$0 \leq \Psi_2 \leq \frac{1}{2}\frac{\log \#k_2}{n_2} = \frac{1}{2}\log(2).$$

where the final equality follows from the fact that $n_2 = 4$ and $\#k_2 = 2^4 = 16$, which one can deduce using a little number theory.
For the Archimedean case, the CPS method computed the following bounds correct to a tolerance of 0.0001,

$$-0.8173... \leq \Psi_{\infty_1} \leq 0.0507...$$
$$-0.8267... \leq \Psi_{\infty_2} \leq 0.0529...$$

which took approximately one minute to compute. If we instead used Bruin's method, we obtain bounds

$$-0.7180... \leq \Psi_{\infty_1} \leq 0.000....$$
$$-0.7289... \leq \Psi_{\infty_2} \leq 0.0000...$$

correct to 4 decimal places, which took 8 minutes and 41 seconds.
Finally, combining these bounds, where we use the results of Bruin's method for the Archimedean contribution, gives global height difference bounds

$$-0.7235... \leq h - \hat{h} \leq 0.3465...$$

References

[Ber05] Daniel J. Bernstein. Factoring into coprimes in essentially linear time. *J. Algorithms*, 54(1):1–30, jan 2005.

[Bru13] Peter Bruin. Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur les courbes elliptiques sur $\overline{\mathbb{Q}}$. *Acta Arith.*, 160(4):385–397, 2013.

[CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union.* London Mathematical Society, 2010.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics.* Springer-Verlag, Berlin, 1993.

[CPS06] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[Cre97] J. E Cremona. *Algorithms for modular elliptic curves / J.E. Cremona.* Cambridge University Press, Cambridge, 2nd ed. edition, 1997.

[Las82] Michael Laska. An algorithm for finding a minimal Weierstrass equation for an elliptic curve. *Math. Comp.*, 38(157):257–260, 1982.

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2024. [Online; accessed 10 April 2024].

[MM97] Henry McKean and Victor Moll. *Theta Functions*, page 125–158. Cambridge University Press, 1997.

[MS16] J. Steffen Müller and Michael Stoll. Computing canonical heights on elliptic curves in quasi-linear time. *LMS J. Comput. Math.*, 19:391–405, 2016.

[SIK95] SAMIR SIKSEK. Infinite descent on elliptic curves. *The Rocky Mountain Journal of Mathematics*, 25(4):1501–1538, 1995.

[Sil88] Joseph H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil97] Joseph H. Silverman. Computing canonical heights with little (or no) factorization. *Mathematics of Computation*, 66(218):787–805, 1997.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Uch08] Yukihiro Uchida. The difference between the ordinary height and the canonical height on elliptic curves. *Journal of Number Theory*, 128:263–279, 2008.