MATHEMATICS OF COMPUTATION
Volume 79, Number 272, October 2010, Pages 2431–2449
S 0025-5718(10)02352-5
Article electronically published on April 12, 2010

COMPUTING A LOWER BOUND FOR THE CANONICAL HEIGHT ON ELLIPTIC CURVES OVER NUMBER FIELDS

THOTSAPHON THONGJUNTHUG

Abstract. Computing a lower bound for the canonical height is a crucial step in determining a Mordell–Weil basis for elliptic curves. This paper presents an algorithm for computing such a lower bound for elliptic curves over number fields without searching for points. The algorithm is illustrated by some examples.

1. Introduction

Let E be an elliptic curve defined over a number field K, and let $E_{\mathrm{tors}}(K)$ be the torsion subgroup of $E(K)$. The *canonical height* on E/K is a quadratic form $\hat{h} : E(K) \to [0, \infty)$ which is positive definite on the lattice $E(K)/E_{\mathrm{tors}}(K)$. Thus there exists a positive lower bound for $\hat{h}(P)$ among all non-torsion $P \in E(K)$.

Computing such a lower bound has a number of applications in arithmetic geometry. In particular, it is a crucial step in determining a Mordell–Weil basis for $E(K)$ (see [7] for full details). In summary, one starts with some points $P_1, \ldots, P_r$ which generate a subgroup of finite index of $E(K)/E_{\mathrm{tors}}(K)$. Using the geometry of numbers [7, Theorem 3.1], this yields an upper bound for the index

$$n = [E(K)/E_{\mathrm{tors}}(K) : \langle P_1, \ldots, P_r \rangle].$$

It follows from the geometry of numbers that, in order to obtain a *smaller* upper bound for n, one must obtain a *larger* lower bound for the canonical height.

Lang's conjecture states (see [8, Conjecture VIII.9.9]) that there exists a constant c_K, depending only on K, such that

$$\hat{h}(P) \geq c_K \log \mathcal{N}(\mathcal{D}_{E/K})$$

for all non-torsion $P \in E(K)$, where $\mathcal{D}_{E/K}$ is the minimal discriminant of E/K, and $\mathcal{N}$ denotes the norm of an integral ideal of K. A result similar to this has been proven [5, Theorem 0.3], although the lower bound obtained by that result is too small for practical use; see Example 10.1 for more details.

In this paper, we present an alternative method for determining a lower bound for $\hat{h}(P)$ without searching for points. This work, which is part of the author's doctoral thesis, is an extension of the author's previous algorithm [11] for elliptic curves over totally real number fields. The methodology is mainly inspired by the algorithm of Cremona and Siksek [2] for the case $K = \mathbb{Q}$. Whereas the structure of this paper will be similar to [11], the novelty comes from a newly added section on the

Received by the editor December 19, 2009 and, in revised form, August 15, 2009.
2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11Y16, 11Y40.
Key words and phrases. Elliptic curves, canonical height, lower bound, number fields.

contributions of the complex embeddings and a repeated quadrisection technique. For more background, the reader should refer to [11].

2. Points of good reduction

Suppose E/K is given by a Weierstrass model

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

with $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K. Let Δ be the discriminant of E. Denote the sets of real and complex archimedean places by M_K^{r} and M_K^{c}, respectively, and let M_K be the set of all places of K. Define the map

$$\phi : E(K) \to \prod_{v \in S} E^{(v)}(K_v)$$

with $S = M_K^{\mathrm{r}} \cup M_K^{\mathrm{c}} \cup \{\mathfrak{p} : \mathfrak{p} \mid \Delta\}$, in such a way that $P \in E(K)$ is mapped into its corresponding point on:

- the real embedding $E^{(v)}(\mathbb{R})$, for each $v \in M_K^{\mathrm{r}}$, and
- the complex embedding $E^{(v)}(\mathbb{C})$, for each $v \in M_K^{\mathrm{c}}$, and
- the minimal model $E^{(v)}(K_v)$, for each non-archimedean place $v \mid \Delta$.

If the class number of K is greater than 1, then $E^{(v)}$ may differ for different non-archimedean places v. In other words, E may not be *globally minimal*.

Instead of working directly on $E(K)$, our method is to determine a positive lower bound μ for the canonical height on the subgroup

$$E_{\mathrm{gr}}(K) = \phi^{-1}\left(\prod_{v \in S} E_0^{(v)}(K_v)\right)$$

where $E_0^{(v)}(K_v)$ is the connected component of the identity. For non-archimedean v, this is the set of points of good reduction. Let c be the least common multiple of the Tamagawa indices

$$c_v = [E^{(v)}(K_v) : E_0^{(v)}(K_v)]$$

for all $v \in M_K$. Note that c is well-defined since $c_v = 1$ for all $v \notin S$. If such μ is determined, then we have

$$\hat{h}(P) > \mu/c^2$$

for all non-torsion $P \in E(K)$, since clearly $cP \in E_{\mathrm{gr}}(K)$, and $\hat{h}$ is quadratic.

In this paper, we will first derive an explicit formula for computing μ. The value of μ obtained by this formula, in practice, will not be as good as the one obtained by the algorithm to be derived later on. The algorithm will check using a number of criteria whether a given $\mu > 0$ is a lower bound on $E_{\mathrm{gr}}(K)$. By repeating the algorithm, we can refine μ further until a sufficient degree of accuracy is achieved.

3. Heights

Note that normalisation of heights varies in literature. In this paper, the local and canonical heights are defined with respect to the divisor $2(O)$, where O is the identity of $E(K)$. This has the same normalisation as the one used in the computer package MAGMA, and gives double the values compared with Silverman's paper [9] where heights are defined with respect to (O).

Let b_2, b_4, b_6, b_8, c_4, c_6, and Δ be the standard invariants associated to E (see [8, p. 46]). Let

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

For $v \in M_K$, let $n_v = [K_v : \mathbb{Q}_v]$, and σ_v be the embedding of K into K_v. For $x \in K$, the *absolute value* of x at v is given by

$$|x|_v = \begin{cases} |\sigma_v(x)| & \text{if } v \in M_K^{\mathrm{r}} \cup M_K^{\mathrm{c}}, \\ \mathcal{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)/n_{\mathfrak{p}}} & \text{if } v = \mathfrak{p}, \end{cases}$$

where $\mathfrak{p}$ is the prime ideal associated to a non-archimedean place v. It is a standard fact that this definition satisfies all axioms of valuation theory and the product formula $\prod_{v \in M_K} |x|_v^{n_v} = 1$. Define

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

Then it can be shown (see e.g. [11, p. 142]) that

$$\hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P) \tag{3.1}$$

where

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

The function $\lambda_v : E(K_v) \to \mathbb{R}$ is called the *local height* at v. This therefore allows us to obtain $\hat{h}(P)$ by computing $\lambda_v(P)$ on each local model $E(K_v)$, noting that $\lambda_v(P) = 0$ for almost all v.

3.1. **The non-archimedean local heights.** For $P \in E(K)$, let $P^{(\mathfrak{p})}$ be the corresponding point of P on the minimal model $E^{(\mathfrak{p})}$. Let Δ and $\Delta^{(\mathfrak{p})}$ be the discriminants of E and $E^{(\mathfrak{p})}$, respectively. If $\langle x(P^{(\mathfrak{p})}) \rangle = AB^{-1}$ for some coprime integral ideals A, B, then we write $\mathrm{denom}(x(P^{(\mathfrak{p})})) = B$.

The following lemma yields a simplified formula for computing the sum of all non-archimedean local heights on $E_{\mathrm{gr}}(K)$.

Lemma 3.1. *Suppose $P \in E_{\mathrm{gr}}(K) \setminus \{O\}$. Then*

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}} \lambda_{\mathfrak{p}}(P) = L(P) - \frac{1}{6} \log \mathcal{N}(M_E)$$

where

$$L(P) = \log \mathcal{N} \left(\prod_{\mathfrak{p} | \mathrm{denom}(x(P^{(\mathfrak{p})}))} \mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(x(P^{(\mathfrak{p})}))} \right), \quad M_E = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}.$$

Note that $\mathcal{N}(M_E) = 1$ if E is a globally minimal model.

Proof. This is a well-known result; see e.g. [11, Lemma 3] for more details. Note that the definition that we use of local height of a point with good reduction does not include a multiple of $-\log |\Delta^{(\mathfrak{p})}|_{\mathfrak{p}}$ (cf. [9, p. 351]). □

3.2. **The archimedean local heights.** For $v \in M_K^{\mathrm{r}} \cup M_K^{\mathrm{c}}$, define α_v by

$$\alpha_v^{-3} = \inf_{P \in E_0^{(v)}(K_v)} \Phi_v(P).$$

These α_v can be computed rapidly by the method in [4, Section 7 and Section 9].

The following lemma, which is Lemma 4 of [11], gives us an estimate for the archimedean local heights.

Lemma 3.2. *If $P \in E_0^{(v)}(K_v) \setminus \{O\}$, then*

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

4. Multiplication by n

In this section, we will derive a lower estimate for the contribution that multiplication by n makes towards $\hat{h}(nP)$.

Let $k_{\mathfrak{p}}$ be the residue class field of $\mathfrak{p}$, and let $e_{\mathfrak{p}}$ be the exponent of the group $E_{\mathrm{ns}}^{(\mathfrak{p})}(k_{\mathfrak{p}}) \cong E_0^{(\mathfrak{p})}(K_{\mathfrak{p}})/E_1^{(\mathfrak{p})}(K_{\mathfrak{p}})$. Define

$$D_E(n) = \sum_{\substack{\mathfrak{p} \text{ prime} \\ e_{\mathfrak{p}} | n}} 2(1 + \mathrm{ord}_{c(\mathfrak{p})}(n/e_{\mathfrak{p}})) \log \mathcal{N}(\mathfrak{p})$$

where $c(\mathfrak{p})$ is the characteristic of $k_{\mathfrak{p}}$. Note that $k_{\mathfrak{p}}$ is a finite field, so $c(\mathfrak{p})$ is always a prime number. In particular, $\mathcal{N}(\mathfrak{p}) = |k_{\mathfrak{p}}| \leq c(\mathfrak{p})^{[K:\mathbb{Q}]}$.

Proposition 4.1. *If $e_{\mathfrak{p}} \mid n$, then we have the following:*

1. *$\mathcal{N}(\mathfrak{p}) \leq (n+1)^{\max\{2,[K:\mathbb{Q}]\}}$. In other words, $D_E(n)$ is finite.*
2. *Moreover, if P is a non-torsion point in $E_{\mathrm{gr}}(K)$ and $n \geq 1$, then*

$$L(nP) \geq D_E(n).$$

Proof. See [11, Proposition 1]. Note that there is one typographical error in that proposition. The correct one should read as follows: if $E^{(\mathfrak{p})}$ has bad reduction at $\mathfrak{p}$, then $e_{\mathfrak{p}}$ is $\mathcal{N}(\mathfrak{p})+1$ or $\mathcal{N}(\mathfrak{p})-1$ according as $E^{(\mathfrak{p})}$ has non-split or split multiplicative reduction at $\mathfrak{p}$. This error, however, does not affect the proof. □

5. A bound for multiples of points of good reduction

We now wish to determine whether a given $\mu > 0$ satisfies $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. To do this, we shall use Proposition 4.1 to obtain a bound for the x-coordinates of the multiples nP.

For $\mu > 0$ and $n \in \mathbb{Z}^+$, define $B_n(\mu)$ by

$$\log B_n(\mu) = [K:\mathbb{Q}]n^2\mu - D_E(n) + \frac{1}{6}\log \mathcal{N}(M_E) + \sum_{v \in M_K^{\mathrm{r}}} \log \alpha_v + 2 \sum_{v \in M_K^{\mathrm{c}}} \log \alpha_v.$$

Proposition 5.1. *If $B_n(\mu) < 1$, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. If $B_n(\mu) \geq 1$, then for all non-torsion $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$, we have*

$$|x(nP)|_v \leq \begin{cases} B_n(\mu) & \text{if } v \in M_K^{\mathrm{r}}, \\ \sqrt{B_n(\mu)} & \text{if } v \in M_K^{\mathrm{c}}. \end{cases}$$

Proof. Suppose $P \in E_{\mathrm{gr}}(K)$ is a non-torsion point with $\hat{h}(P) \le \mu$. By Lemma 3.2, we have

$$\log \max\{1, |x(nP)|_v\} - \lambda_v(nP) \le \log \alpha_v$$

for all $v \in M_K^{\mathrm{r}} \cup M_K^{\mathrm{c}}$. This implies that

$$\begin{aligned}(5.1)\qquad &\sum_{v \in M_K^{\mathrm{r}}} \log \max\{1, |x(nP)|_v\} + 2 \sum_{v \in M_K^{\mathrm{c}}} \log \max\{1, |x(nP)|_v\} \\ &\qquad \le \sum_{v \in M_K^{\mathrm{r}}} \lambda_v(nP) + 2 \sum_{v \in M_K^{\mathrm{c}}} \lambda_v(nP) + \sum_{v \in M_K^{\mathrm{r}}} \log \alpha_v + 2 \sum_{v \in M_K^{\mathrm{c}}} \log \alpha_v.\end{aligned}$$

Note that $n_v = 1$ for all $v \in M_K^{\mathrm{r}}$ and $n_v = 2$ for all $v \in M_K^{\mathrm{c}}$. By writing $\hat{h}(nP)$ as a sum of local heights (3.1), we have

$$\begin{aligned}&\sum_{v \in M_K^{\mathrm{r}}} \lambda_v(nP) + 2 \sum_{v \in M_K^{\mathrm{c}}} \lambda_v(nP) = [K : \mathbb{Q}]\hat{h}(nP) - \sum_{\mathfrak{p}} n_{\mathfrak{p}} \lambda_{\mathfrak{p}}(nP) \\ &= [K : \mathbb{Q}]\hat{h}(nP) - L(P) + \frac{1}{6}\log \mathcal{N}(M_E) && \text{by Lemma 3.1} \\ &\le [K : \mathbb{Q}]\hat{h}(nP) - D_E(n) + \frac{1}{6}\log \mathcal{N}(M_E) && \text{by Proposition 4.1(2)} \\ &\le [K : \mathbb{Q}]n^2\mu - D_E(n) + \frac{1}{6}\log \mathcal{N}(M_E) && \text{since } \hat{h}(P) \le \mu.\end{aligned}$$

Combining this with (5.1) and taking the exponential, we obtain

$$\left(\prod_{v \in M_K^{\mathrm{r}}} \max\{1, |x(nP)|_v\}\right)\left(\prod_{v \in M_K^{\mathrm{c}}} \max\{1, |x(nP)|_v\}^2\right) \le B_n(\mu).$$

But the left-hand side is at least 1. Thus, if $B_n(\mu) < 1$, then we have a contradiction, i.e. $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. On the other hand, it can be seen that $|x(nP)|_v \le B_n(\mu)$ for all $v \in M_K^{\mathrm{r}}$, and $|x(nP)|_v^2 \le B_n(\mu)$ for all $v \in M_K^{\mathrm{c}}$. □

We now give an explicit formula for a lower bound on $E_{\mathrm{gr}}(K)$.

Theorem 5.2. *Let $\mathfrak{p}$ be a prime ideal such that*

$$(5.2)\qquad \mathcal{N}(\mathfrak{p}) > \left(\prod_{v \in M_K^{\mathrm{r}}} \sqrt{\alpha_v}\right)\left(\prod_{v \in M_K^{\mathrm{c}}} \alpha_v\right)\mathcal{N}(M_E)^{\frac{1}{12}}.$$

Set $n = e_{\mathfrak{p}}$ and

$$\mu_0 = \frac{1}{[K : \mathbb{Q}]n^2}\left(D_E(n) - \sum_{v \in M_K^{\mathrm{r}}} \log \alpha_v - 2 \sum_{v \in M_K^{\mathrm{c}}} \log \alpha_v - \frac{1}{6}\log \mathcal{N}(M_E)\right).$$

Then $\mu_0 > 0$, and $\hat{h}(P) \ge \mu_0$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.

Proof. This can be proved in a similar way as in [11, Corollary 1]. □

Although it is possible to obtain a lower bound on $E_{\mathrm{gr}}(K)$ by Theorem 5.2 alone, our practical experience shows that this bound is not as good as the one obtained by collecting more information on $x(nP)$. This will be illustrated in Example 10.1.

6. Solving inequalities I: Real embeddings

Proposition 5.1 allows us to solve a system of inequalities on each embedding $E^{(v)}$. In this section, we will first concentrate on solving a system of inequalities on each real embedding $E^{(v)}(\mathbb{R})$, i.e. for $v \in M_K^{\mathrm{r}}$.

If $B_n(\mu) \geq 1$, then Proposition 5.1 says that all non-torsion $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$ must satisfy $|x(nP)|_v \leq B_n(\mu)$ for every $v \in M_K^{\mathrm{r}}$. Let $\sigma_v : K \to \mathbb{R}$ be the real embedding associated to v. This means that we need to consider $\sigma_v(nP)$ over $E_0^{(v)}(\mathbb{R})$, where $E^{(v)}$ is given by

$$E^{(v)}: \quad y^2 + \sigma_v(a_1)xy + \sigma_v(a_3)y = x^3 + \sigma_v(a_2)x^2 + \sigma_v(a_4)x + \sigma_v(a_6).$$

To prove that $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$, we attempt to derive a contradiction from these inequalities using an application of the *elliptic logarithm*.

6.1. **Elliptic logarithm.**

This is explained in full detail in [11, Section 5.1], but for convenience we shall cover it briefly.

The elliptic logarithm is an isomorphism of real analytic Lie groups $\varphi : E_0(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}$. This can be rapidly computed by the method of arithmetic-geometric mean (see e.g. [1, Algorithm 7.4.8]). We wish to apply the elliptic logarithm to solve our inequalities on each real embedding $E^{(v)}(\mathbb{R})$. For convenience, we shall identify $\mathbb{R}/\mathbb{Z}$ with the interval $[0, 1)$.

The process can be described roughly as follows: let $\varphi_v : E_0^{(v)}(\mathbb{R}) \to [0, 1)$ be the elliptic logarithm associated to the real embedding $E^{(v)}$. Suppose $P \in E_0^{(v)}(\mathbb{R})$ satisfies $\xi_1 \leq |x(P)| \leq \xi_2$. Then this is equivalent to

$$\varphi_v(P) \in \mathcal{S}^{(v)}(\xi_1, \xi_2)$$

where $\mathcal{S}^{(v)}(\xi_1, \xi_2)$ is a disjoint union of subintervals of $[0, 1)$ depending on ξ_1, ξ_2.

If $\bigcup[a_i, b_i]$ is a disjoint union of intervals and $\alpha \in \mathbb{R}$, we define

$$\alpha + \bigcup[a_i, b_i] = \bigcup[a_i + \alpha, b_i + \alpha], \quad \alpha \bigcup[a_i, b_i] = \bigcup[\alpha a_i, \alpha b_i] \quad (\text{for } \alpha > 0).$$

Lemma 6.1. *Suppose $\xi_1 \leq \xi_2$, and $n \in \mathbb{Z}^+$. Let*

$$\mathcal{S}_n^{(v)}(\xi_1, \xi_2) = \bigcup_{\alpha=0}^{n-1} \left(\frac{\alpha}{n} + \frac{1}{n} \mathcal{S}^{(v)}(\xi_1, \xi_2) \right).$$

Then $P \in E_0^{(v)}(\mathbb{R})$ satisfies $\xi_1 \leq x(nP) \leq \xi_2$ if and only $\varphi_v(P) \in \mathcal{S}_n^{(v)}(\xi_1, \xi_2)$.

Proof. See [11, Proposition 3]. □

This together with Proposition 5.1 leads to the following proposition.

Proposition 6.2. *If $B_n(\mu) < 1$ for some $n \in \mathbb{Z}^+$, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. If $B_n(\mu) \geq 1$ for all $n = 1, \ldots, n_{\max}$, then every non-torsion point $P \in E_{\mathrm{gr}}(K)$ with $h(P) \leq \mu$ satisfies*

$$\varphi_v(\sigma_v(P)) \in \bigcap_{n=1}^{n_{\max}} \mathcal{S}_n^{(v)}(-B_n(\mu), B_n(\mu))$$

for every $v \in M_K^{\mathrm{r}}$. In particular, if the intersection is empty for some $v \in M_K^{\mathrm{r}}$, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.

7. Solving inequalities II: Complex embeddings

Suppose $B_n(\mu) \geq 1$. Proposition 5.1 also says that all non-torsion $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$ satisfy $|x(nP)|_v \leq \sqrt{B_n(\mu)}$ for every $v \in M_K^c$. We will show that each of these inequalities corresponds to a region in the *fundamental parallelogram*, and solving this system of inequalities is equivalent to intersecting all such regions. Most of our work is devoted to this section.

7.1. **Fundamental parallelograms.** Let $\Lambda \subset \mathbb{C}$ be a lattice generated by periods $\omega_1, \omega_2 \in \mathbb{C}$ with $\omega_2/\omega_1 \notin \mathbb{R}$. The *(closed) fundamental parallelogram* of Λ is the set

$$\Pi_{\omega_1,\omega_2} = \{\lambda_1\omega_1 + \lambda_2\omega_2 : 0 \leq \lambda_1, \lambda_2 \leq 1\}.$$

Let $E^{(v)}$ be the complex embedding of E associated to $v \in M_K^c$. It is well known that there exists a complex analytic group isomorphism $\varphi_v : E^{(v)}(\mathbb{C}) \to \mathbb{C}/\Lambda$, for some lattice Λ generated by ω_1, ω_2 satisfying the above condition. Note that every element of $\mathbb{C}/\Lambda$ has a representative in Π_{ω_1,ω_2} which is unique except for points on the boundary of Π_{ω_1,ω_2}. After choosing a lift in Π_{ω_1,ω_2} for each $P \in E^{(v)}(\mathbb{C})$, we may view φ_v as a map $E^{(v)}(\mathbb{C}) \to \Pi_{\omega_1,\omega_2} \subset \mathbb{C}$. Let $\tau = \omega_2/\omega_1$. Without loss of generality, we may choose the basis ω_1, ω_2 such that

$$|\Re(\tau)| \leq 1/2 \quad \text{and} \quad |\tau| \geq 1.$$

Let Λ_τ be the lattice generated by $1, \tau$. Then clearly the map $\delta : \mathbb{C} \to \mathbb{C}$ given by $z \mapsto z/\omega_1$ induces a bijection $\Lambda \to \Lambda_\tau$. Denote $\Pi_{1,\tau}$ by Π_τ, and let

$$\mathcal{H}_\tau = \{\lambda_1 + \lambda_2\tau : 0 \leq \lambda_1 \leq 1,\ 0 \leq \lambda_2 \leq 1/2\}$$

(i.e. $\mathcal{H}_\tau$ is the lower half of Π_τ). Each $P \in E^{(v)}(\mathbb{C})$ maps to a point $z \in \Pi_\tau$, and either P or $-P$ maps to a point in $\mathcal{H}_\tau$. Hence we can let

$$\psi_v(P) = \begin{cases} \psi_v'(P) & \text{if } \psi_v'(P) \in \mathcal{H}_\tau, \\ \psi_v'(-P) & \text{if } \psi_v'(P) \notin \mathcal{H}_\tau, \end{cases} \tag{7.1}$$

where $\psi_v' = \delta \circ \varphi_v$ (viewed as a map $E^{(v)}(\mathbb{C}) \to \Pi_\tau$), so that in all cases $\psi_v(P) \in \mathcal{H}_\tau$.

7.2. **The corresponding region.** In this section, we will give a description of a region in $\mathcal{H}_\tau$ that corresponds to an inequality on $|x(P)|_v$.

Suppose $E^{(v)}$ is given by the Weierstrass equation

$$E^{(v)} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{C}$. Let ω_1, ω_2, and τ be as above. Recall that we have the Weierstrass parameterisation $\mathbb{C}/\Lambda_\tau \tilde{\to} E_W(\mathbb{C})$, where E_W is the elliptic curve $Y^2 = 4X^3 - g_2(\Lambda_\tau)X - g_3(\Lambda_\tau)$, given by

$$z \mapsto (\wp_{\Lambda_\tau}(z), \wp'_{\Lambda_\tau}(z)).$$

Moreover, we have an isomorphism $E_W(\mathbb{C}) \to E^{(v)}(\mathbb{C})$ given by

$$(X, Y) \mapsto (x, y) = \left(\omega_1^{-2}X - \frac{b_2}{12}, \frac{\omega_1^{-3}Y - a_1x - a_3}{2}\right).$$

Hence for any $\xi \geq 0$, it is clear that

$$|x| \leq \xi \iff |\wp_{\Lambda_\tau}(z)| \leq U_\xi$$

where $U_\xi = |\omega_1|^2 (\xi + |b_2|/12)$.

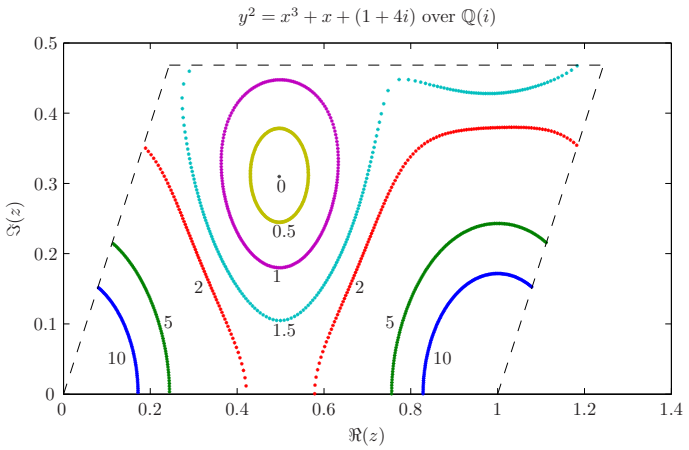

FIGURE 1. The boundary on $\mathcal{H}_\tau$ associated to different U_ξ. Each curve is labelled by the relevant value of ξ.

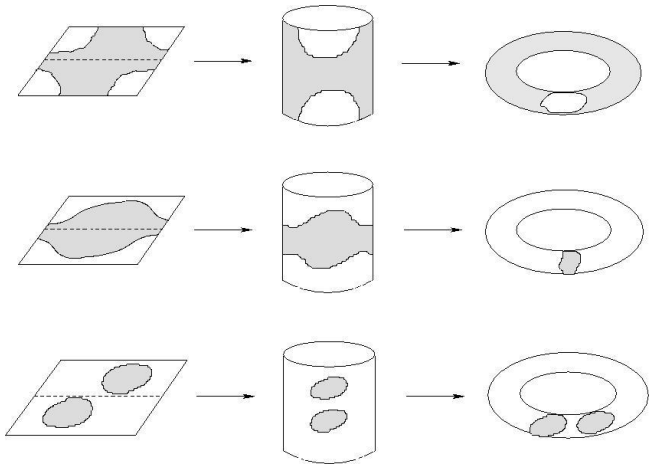

FIGURE 2. Loops on the torus $\mathbb{C}/\Lambda_\tau$ when the boundary varies.

Now we can consider the set

$$\ell = \{z \in \mathcal{H}_\tau : |\wp_{\Lambda_\tau}(z)| = U_\xi\}$$

as a curve[1] on $\mathcal{H}_\tau$ (see Figure 1). This is the boundary of the region

$$\mathcal{R}^{(v)}(\xi) = \{z \in \mathcal{H}_\tau : |\wp_{\Lambda_\tau}(z)| \leq U_\xi\}.$$

Since the Weierstrass $\wp$-function becomes a one-to-one continuous map once its domain is restricted to $\mathcal{H}_\tau$, the equation $|\wp_{\Lambda_\tau}(z)| = U_\xi$ yields only one curve on $\mathcal{H}_\tau$. By symmetry (about the mid-point of Π_τ), we also have another identical boundary on the upper half of Π_τ. Depending on U_ξ, the boundaries on both halves topologically form either one or two identical loops on the torus $\mathbb{C}/\Lambda_\tau$, as shown in Figure 2.

[1]This may have either one or two connected components on $\mathcal{H}_\tau$.

7.3. **Determining the region.** For practical reasons we prefer to approximate $\mathcal{R}^{(v)}$ by a finite number of parallelograms whose union covers $\mathcal{R}^{(v)}$. Denote by $\mathcal{S}^{(v)}$ the finite set of these parallelograms. A finer approximation to $\mathcal{R}^{(v)}$ can be obtained by decreasing the size of parallelograms in $\mathcal{S}^{(v)}$.

The construction of $\mathcal{S}^{(v)}$ will be explained in detail in Section 7.3.3. For now we mention that $\mathcal{S}^{(v)}(\xi)$ has the following properties:

(1) $\bigcup_{C\in\mathcal{S}^{(v)}(\xi)} C \supseteq \mathcal{R}^{(v)}(\xi)$, i.e. the union of all parallelograms in $\mathcal{S}^{(v)}(\xi)$ contains the actual region $\mathcal{R}^{(v)}(\xi)$.
(2) Every $C \in \mathcal{S}^{(v)}(\xi)$ contains z such that $|\wp_{\Lambda_\tau}(z)| \le U_\xi$. In other words, $C \cap \mathcal{R}^{(v)}(\xi) \neq \emptyset$ for all $C \in \mathcal{S}^{(v)}(\xi)$.

7.3.1. *Approximating the Weierstrass $\wp$-function.* Let $q = \exp(2\pi i\tau)$ and $u = \exp(2\pi iz)$. For $k \in \mathbb{Z}$, we define the function $f_k(z,\tau)$ by

$$\frac{f_k(z,\tau)}{(2\pi i)^2} = \frac{u}{(1-u)^2} + \frac{1}{12} + \sum_{n=1}^{k-1}\left[\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - \frac{2q^n}{(1-q^n)^2}\right].$$

In particular, $\lim_{k\to\infty} f_k(z,\tau) = \wp_{\Lambda_\tau}(z)$ for all non-lattice points z (see [1, Proposition 7.4.4]). By choosing a suitable k, we can bound the error which occurs when $|f_k(z,\tau)|$ is used as the approximation to $|\wp_{\Lambda_\tau}(z)|$, as shown in the next lemma.

Lemma 7.1. *Suppose $z \in \mathcal{H}_\tau$ with $z \neq 0, 1$. Let $\alpha = \Im(z)/\Im(\tau)$. Then*

$$\big||\wp_{\Lambda_\tau}(z)| - |f_k(z,\tau)|\big| \le \frac{4\pi^2}{1-|q|}\left[\frac{|q|^{k+\alpha}}{(1-|q|^{k+\alpha})^2} + \frac{|q|^{k-\alpha}}{(1-|q|^{k-\alpha})^2} + \frac{2|q|^k}{(1-|q|^k)^2}\right].$$

Proof. First we have

$$\wp_{\Lambda_\tau}(z) - f_k(z,\tau) = (2\pi i)^2 \sum_{n=k}^{\infty}\left[\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - \frac{2q^n}{(1-q^n)^2}\right].$$

Observe that $|u| = |q|^\alpha$. By the triangle inequality, we obtain

$$\frac{|\wp_{\Lambda_\tau}(z) - f_k(z,\tau)|}{4\pi^2} \le \sum_{n=k}^{\infty}\left[\frac{|q|^{n+\alpha}}{(1-|q|^{n+\alpha})^2} + \frac{|q|^{n-\alpha}}{(1-|q|^{n-\alpha})^2} + \frac{2|q^n|}{(1-|q^n|)^2}\right]. \tag{7.2}$$

Since we work on $\mathcal{H}_\tau$, we have $|q| < 1$ and $0 \le \alpha \le 1/2$, which implies that $|q|^{n\pm\alpha} < 1$ for all $n \ge 1$. Thus we have the estimate

$$\sum_{n=k}^{\infty}\frac{|q|^{n\pm\alpha}}{(1-|q|^{n\pm\alpha})^2} \le \frac{1}{(1-|q|^{k\pm\alpha})^2}\sum_{n=k}^{\infty}|q|^{n\pm\alpha} \le \frac{|q|^{k\pm\alpha}}{(1-|q|^{k\pm\alpha})^2(1-|q|)},$$

and similarly

$$\sum_{n=k}^{\infty}\frac{2|q|^n}{(1-|q|^n)^2} \le \frac{2|q|^k}{(1-|q|^k)^2(1-|q|)}.$$

This together with (7.2) and the triangle inequality yields the result. □

It is readily verified that the absolute error given by Lemma 7.1 attains its maximum when $\alpha = 1/2$, and becomes smaller as k increases. Moreover, it can be seen that this absolute error decreases as $\Im(\tau)$ increases.

Recall that every parallelogram C in $\mathcal{S}^{(v)}(\xi)$ satisfies $|\wp_{\Lambda_\tau}(z)| \le U_\xi$ for some $z \in C$. In practice, we can compute $|f_k(z,\tau)|$ and add it with the error given by Lemma 7.1 to obtain a (small) interval which contains $|\wp_{\Lambda_\tau}(z)|$. On each of the

four line segments comprising the boundary of C, we can parameterize $|f_k(z,\tau)|$ by a real-valued function $f_k(x,\tau)$ or $f_k(y,\tau)$, where $x = \Re(z)$ and $y = \Im(z)$. We wish to find the range of f_k when x or y varies along the line. For this computation, we find some techniques from *interval arithmetic* (see [6]) to be very useful.

7.3.2. *Interval arithmetic on $f_k(z,\tau)$.* Before we proceed to its application, we shall first explain briefly what interval arithmetic is.

Let $I = [a,b]$ and $J = [c,d]$ (with $a \le b$ and $c \le d$) be two intervals of real numbers. We can define an *arithmetic operation* on intervals by

$$I * J = \{x * y : a \le x \le b,\, c \le y \le d\}$$

where $*$ is an operation on real numbers. A number of usual arithmetic operations on real numbers can be extended to the one on intervals. For example,

$$\begin{aligned} I + J &= [a+c, b+d], \qquad I - J = [a-d, b-c], \\ I \cdot J &= [\min\{ac,ad,bc,bd\}, \max\{ac,ad,bc,bd\}], \\ I/J &= [a,b] \cdot [1/d, 1/c] \quad \text{provided that } 0 \notin J. \end{aligned}$$

It can be seen easily that interval addition and interval multiplication are both associative and commutative. Distributivity, however, does not always hold for interval arithmetic. For example,

$$\begin{aligned} [1,3] \cdot ([1,3] - [1,3]) = [1,3] \cdot [-2,2] &= [-6,6], \text{ whereas} \\ [1,3] \cdot [1,3] - [1,3] \cdot [1,3] = [1,9] - [1,9] &= [-8,8]. \end{aligned}$$

In general, if I, J, K are intervals, then

$$I \cdot (J + K) \subset I \cdot J + I \cdot K.$$

This is normally known as *subdistributivity*.

One important property of interval arithmetic is that it is *inclusion monotonic*, i.e. if $I \subset K$ and $J \subset L$ are intervals, then

$$\begin{aligned} I + J \subset K + L, \quad I - J \subset K - L, \\ I \cdot J \subset K \cdot L, \qquad I/J \subset K/L \quad \text{provided that } 0 \notin L. \end{aligned}$$

This leads to

Theorem 7.2 ([6, Theorem 3.1])**.** *Let $f(X_1,\dots,X_n)$ be a rational expression with real coefficients in the interval variables $X_1,\dots,X_n$, i.e. a finite combination of $X_1,\dots,X_n$ and a finite set of constant intervals with interval arithmetic operations. Then*

$$X_1' \subset X_1,\, \dots,\, X_n' \subset X_n \quad \textit{implies} \quad f(X_1',\dots,X_n') \subset f(X_1,\dots,X_n)$$

for every set of intervals $X_1,\dots,X_n$ for which the interval arithmetic operations in f are defined.

Suppose $f(x_1,\dots,x_n)$ is a real rational expression, i.e. f is a quotient of real polynomials in terms of $x_1,\dots,x_n$. Then by Theorem 7.2, the resulting interval $F = f(X_1,\dots,X_n)$ will always contain the actual range of $f(x_1,\dots,x_n)$ for $x_i \in X_i$. In particular, F will be the actual range of $f(x_1,\dots,x_n)$ for $x_i \in X_i$ if each variable x_i occurs only once in f (note that $x_i^2 = x_i \cdot x_i$ is taken as two occurrences). With some techniques, e.g. using subdistributivity to group common terms in f, the resulting interval F can be made smaller.

Recall the function $f_k(z,\tau)$ in Section 7.3.1. Suppose $z = x+iy \in \mathbb{C}$ is on a fixed line segment L. Depending on L, we can regard z as a function of either x or y (for example, if z is on a vertical line, then x is fixed but y varies). Thus, provided that L is fixed and $z \in L$, we can consider

$$g(z) = |f_k(z,\tau)|^2$$

as a real function of one real variable, i.e. either $g(z) = g(z(x))$ or $g(z) = g(z(y))$, depending on L. To ease notation, we shall write

$$f(*) = g(z(*)),$$

where $*$ is either x or y, depending on how z is parameterized along L.

The next proposition shows that we can apply interval arithmetic to $f(*)$.

Proposition 7.3. *Define $f(*)$ as above. Then f can be extended to a real rational expression of at most three interval variables, depending on the line segment L.*

Proof. First we note that

$$f(*) = |f_k(z,\tau)|^2 = \Re(f_k(z,\tau))^2 + \Im(f_k(z,\tau))^2.$$

We will show how to obtain the real part of $f_k(z,\tau)$, the imaginary part of $f_k(z,\tau)$ can be deduced in a similar way.

The real part of $f_k(z,\tau)$ consists of the real parts of the terms

$$\frac{u}{(1-u)^2}, \quad \frac{1}{12}, \quad \frac{q^n u}{(1-q^n u)^2}, \quad \frac{q^n u^{-1}}{(1-q^n u^{-1})^2}, \quad \frac{q^n}{(1-q^n)^2} \tag{7.3}$$

where $u = \exp(2\pi i z)$ and $q = \exp(2\pi i \tau)$. Write $z = x + iy$. Let

$$x_1 = \exp(-2\pi y), \quad x_2 = \cos(2\pi x), \quad x_3 = \sin(2\pi x).$$

Consider the following two cases:

(1) **If L is a non-vertical line** (i.e. $y = \alpha x + \beta$ for some finite α and β), then

$$\Re\left(\frac{u}{(1-u)^2}\right) = \frac{x_1 x_2 (1+x_1^2) - 2x_1^2}{(1 - 2x_1 x_2 + x_1^2)^2}.$$

Similarly, it can be shown that the real parts of the other terms in (7.3) can be written as rational expressions in terms of x_1, x_2, x_3.

(2) **If L is a vertical line** (i.e. x is fixed), then we have $\Re(u/(1-u)^2)$ as above. Since x_2 and x_3 are now constant, we have $\Re(u/(1-u)^2)$ as a rational expression in terms of x_1 only. This is also the case for the real parts of the other terms in (7.3).

Thus we have $f(*)$ as a real rational expression in terms of x_1, x_2, x_3. Suppose that $a \le x \le b$ and $c \le y \le d$ on L (note that $c, d \ge 0$ since we work on $\mathcal{H}_\tau$). Let

$$\begin{aligned} X_1 = \exp(-2\pi[c,d]) &= [\exp(-2\pi d), \exp(-2\pi c)], \\ X_2 = \cos(2\pi[a,b]) &= [\min_{a\le x\le b} \cos(2\pi x), \max_{a\le x\le b} \cos(2\pi x)], \\ X_3 = \sin(2\pi[a,b]) &= [\min_{a\le x\le b} \sin(2\pi x), \max_{a\le x\le b} \sin(2\pi x)]. \end{aligned}$$

After replacing x_1, x_2, x_3 in f with X_1, X_2, X_3, respectively, we finally obtain the interval version of f. □

Since $f(X_1, X_2, X_3)$ is a real rational expression of interval variables, then Theorem 7.2 applies. Together with the error term in Lemma 7.1, this easily yields

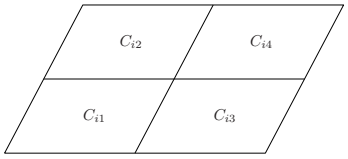

FIGURE 3. Four quarters of C_i.

Proposition 7.4. *Let L be a line segment in the complex plane. Define X_1, X_2, X_3 to be the intervals depending on L as above.*

Let $[u_1, u_2] = f(X_1, X_2, X_3)$ (with $u_2 \geq u_1 \geq 0$). For a fixed $k \in \mathbb{Z}^+$, let $\epsilon = \epsilon_k$ be the maximum absolute error given by Lemma 7.1. Then for all $z \in L$, we have

$$\sqrt{u_1} - \epsilon \leq |\wp_{\Lambda_\tau}(z)| \leq \sqrt{u_2} + \epsilon.$$

7.3.3. *Constructing $\mathcal{S}^{(v)}$.* We are now ready to construct $\mathcal{S}^{(v)}$.

Let L be a line segment in the complex plane. By Proposition 7.4, the interval

$$I(L) = [\sqrt{u_1} - \epsilon, \sqrt{u_2} + \epsilon]$$

contains the actual range of $|\wp_{\Lambda_\tau}(z)|$ where $z \in L$. We can then extend this notion to any parallelogram C by letting

$$I(C) = \bigcup_{L \in \partial C} I(L)$$

where ∂C is the boundary of C. Note that the four intervals $I(L)$ for $L \in \partial C$ will overlap, so $I(C)$ is an interval.

We define $\mathcal{S}^{(v)}(\xi)$ recursively as follows: first we let

$$\mathcal{S}^{(v,0)}(\xi) = \{\mathcal{H}_\tau\}.$$

Suppose $\mathcal{S}^{(v,r)}(\xi) = \{C_1, \ldots, C_m\}$, where $m = 4^r$. Let

$$\mathcal{S}'^{(v,r+1)} = \{C_{11}, \ldots, C_{14}, \ldots, C_{m1}, \ldots, C_{m4} : C_i = \bigcup_{j=1}^{4} C_{ij}\},$$

i.e. $C_{i1}, \ldots, C_{i4}$ are the four quarters of C_i, as shown in Figure 3.

Suppose $E^{(v)}$ is in the form $Y^2 = 4X^3 + AX + B$ for some $A, B \in \mathbb{C}$. Let $P \in E^{(v)}(\mathbb{C})$ be a point with $X(P) = 0$. Let $C_0 \in \mathcal{S}'^{(v,r+1)}$ be the parallelogram containing $\psi_v(P)$ (see (7.1) for the definition of ψ_v). Note that we may have $I(C_0) \cap [0, U_\xi] = \emptyset$. Then we define

$$\mathcal{S}^{(v,r+1)}(\xi) = \{C_0\} \cup \{C \in \mathcal{S}'^{(v,r+1)} : I(C) \cap [0, U_\xi] \neq \emptyset\}.$$

Finally, we let $\mathcal{S}^{(v)}(\xi) = \mathcal{S}^{(v,r)}(\xi)$ for some $r > 0$.

If $\mathcal{S}$ is a set of parallelograms in $\mathbb{C}$, we denote $\bigcup_{C \in \mathcal{S}} C$ by $\bigcup \mathcal{S}$. It is then obvious from the construction above that

$$\bigcup \mathcal{S}^{(v,0)}(\xi) \supset \bigcup \mathcal{S}^{(v,1)}(\xi) \supset \ldots \supset \bigcup \mathcal{S}^{(v,r)}(\xi) \supset \ldots \supset \mathcal{R}^{(v)}(\xi).$$

In practice, we can increase our computational speed by using the following techniques to assist in finding $\mathcal{S}^{(v,r+1)}$.

Lemma 7.5 (Four-Corner Test)**.** *Suppose $C \in \mathcal{S}'^{(v,r+1)}(\xi)$. Let $z_1, \dots, z_4$ be the corners of C, and let ϵ_k be the maximum absolute error given by Lemma* 7.1*. Define*

$$I(z) = [\,|f_k(z,\tau)| - \epsilon_k, |f_k(z,\tau)| + \epsilon_k\,].$$

If $I(z_i) \subset [0, U_\xi]$ for some $i = 1, \dots, 4$, then $C \in \mathcal{S}^{(v,r+1)}(\xi)$.

Proof. This will imply that $|\wp_{\Lambda_\tau}(z)| \le U_\xi$ for some $z \in C$ (namely $z = z_i$). Thus $C \in \mathcal{S}^{(v,r+1)}(\xi)$. □

In practice, checking whether C is in $\mathcal{S}^{(v,r+1)}(\xi)$ by this test is considerably faster than the usual criterion $I(C) \cap [0, U_\xi]$. In addition, most of the parallelograms in $\mathcal{S}^{(v,r+1)}(\xi)$ can be found rapidly by this test.

Lemma 7.6. *For $r \ge 0$, let S_{r+1} be the set of all parallelograms in $\mathcal{S}'^{(v,r+1)}(\xi)$ which satisfy the condition in Lemma* 7.5*. Let*

$$\partial S_{r+1} = \{C \in \mathcal{S}'^{(v,r+1)}(\xi) \setminus S_{r+1} : C \text{ is adjacent to } \bigcup S_{r+1}\}.$$

If $I(C) \cap [0, U_\xi] = \emptyset$ for all $C \in \partial S_{r+1}$, then $\mathcal{S}^{(v,r+1)}(\xi) = S_{r+1}$.

Proof. If all parallelograms in ∂S_{r+1} are excluded from $\mathcal{S}^{(v,r+1)}(\xi)$, then this means there is no part of the boundary ℓ of the actual region $\mathcal{R}^{(v)}(\xi)$ passing through $\bigcup \partial S_{r+1}$. Thus the one-to-one and continuity properties of the Weierstrass $\wp$-function on $\mathcal{H}_\tau$ imply that the boundary ℓ of $\mathcal{R}^{(v)}(\xi)$ lies entirely in $\bigcup S_{r+1}$, and so all parallelograms in $\mathcal{S}'^{(v,r+1)}(\xi) \setminus S_{r+1}$ can be discarded. □

An illustration of using these techniques to construct $\mathcal{S}^{(v)}$ is shown[2] in Figure 4. In this figure, the process of determining $\mathcal{S}^{(v)}$ consists of the following steps:

(1) Starting with $\mathcal{S}'^{(v,r+1)}(\xi)$ for some r, we use Lemma 7.5 to identify a number of parallelograms $C \in \mathcal{S}'^{(v,r+1)}(\xi)$ which are also in $\mathcal{S}^{(v,r+1)}(\xi)$ (these are marked by "*"). Let S_{r+1} be the set of all such parallelograms C.
(2) Identify all parallelograms in ∂S_{r+1} (these are marked by "?").
(3) For each $C \in \partial S_{r+1}$, check if $I(C) \cap [0, U_\xi] = \emptyset$. If so, then $C \notin \mathcal{S}^{(v,r+1)}(\xi)$ and thus can be discarded (this is marked by ".").
(4) If it turns out that the set ∂S_{r+1} is entirely discarded, then by Lemma 7.6 we have $\mathcal{S}^{(v,r+1)}(\xi) = S_{r+1}$. In other words, every parallelogram in $\mathcal{S}'^{(v,r+1)}(\xi) \setminus S_{r+1}$ is discarded. Finally, we let $\mathcal{S}^{(v)}(\xi) = \mathcal{S}^{(v,r+1)}(\xi)$.

7.4. **Division by n.** We have seen that the inequality $|x(P)|_v \le \xi$ yields the region $\bigcup \mathcal{S}^{(v)}(\xi)$ in $\mathcal{H}_\tau$. Since the Weierstrass $\wp$-function is even, we also have another identical region in the upper half of Π_τ. Let $\mathcal{T}^{(v)}(\xi)$ be the union of both regions. Then clearly $\mathcal{T}^{(v)}(\xi)$ contains the set $\{z \in \Pi_\tau : |\wp_{\Lambda_\tau}(z)| \le U_\xi\}$.

Recall the isomorphism $\psi'_v : E^{(v)}(\mathbb{C}) \to \Pi_\tau$. Suppose $P \in E^{(v)}(\mathbb{C})$ is given, and consider all points $Q \in E^{(v)}(\mathbb{C})$ such that $P = nQ$. Let $z = \psi'_v(P)$ and $z' = \psi'_v(Q)$. Then we have

$$z = nz' \pmod{\Lambda_\tau}.$$

In fact, if $z = \alpha + \beta\tau$ for some $0 \le \alpha, \beta \le 1$, then

$$z' \in \left\{ \frac{\alpha + s}{n} + \frac{(\beta + t)\tau}{n} : 0 \le s, t \le n - 1 \right\}.$$

[2]Here $\mathcal{S}^{(v)} = \mathcal{S}^{(v,4)}(0.4)$ for the elliptic curve $y^2 = x^3 + x + (1 + 4i)$ defined over $\mathbb{Q}(i)$.

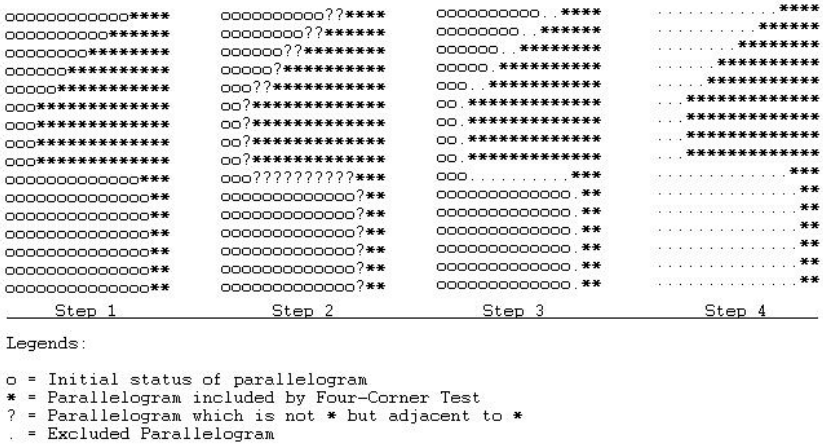

FIGURE 4. Illustration of how to obtain $\mathcal{S}^{(v)}$.

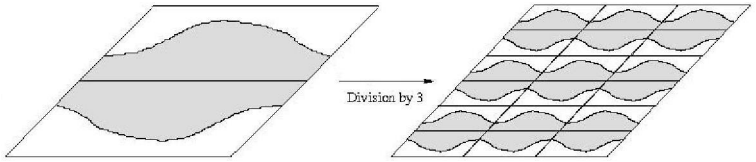

FIGURE 5. Division on Π_τ by 3.

This therefore allows us to "divide" $\mathcal{T}^{(v)}(\xi)$ by n (see Figure 5 for an illustration) to obtain a new region

$$\mathcal{T}_n'^{(v)}(\xi) = \{z' \in \Pi_\tau : nz' \pmod{\Lambda_\tau} \in C, \text{ for some } C \in \mathcal{T}^{(v)}(\xi)\}.$$

Due to the symmetry of $\mathcal{T}_n'^{(v)}$, we can let

$$\mathcal{T}_n^{(v)}(\xi) = \mathcal{T}_n'^{(v)}(\xi) \cap \mathcal{H}_\tau.$$

The following lemma is analogous to Lemma 6.1.

Lemma 7.7. *If $P \in E^{(v)}(\mathbb{C})$ satisfies $|x(nP)| \le \xi$, then $\psi_v(P) \in \mathcal{T}_n^{(v)}(\xi)$.*

Proof. If $|x(nP)| \le \xi$, then we have $\psi_v(nP) \in C$ for some $C \in \mathcal{S}^{(v)}(\xi) \subset \mathcal{T}^{(v)}(\xi)$. Since $n\psi_v(P)$ is either $\psi_v(nP)$ or $-\psi_v(nP) \pmod{\Lambda_\tau}$, in any case we have $\psi_v(P) \in \mathcal{T}_n'^{(v)}(\xi) \cap \mathcal{H}_\tau = \mathcal{T}_n^{(v)}(\xi)$. □

Together with Proposition 5.1, we have

Proposition 7.8. *If $B_n(\mu) \ge 1$ for all $n = 1, \dots, n_{\max}$, then every non-torsion point $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \le \mu$ satisfies*

$$\psi_v(\sigma_v(P)) \in \bigcap_{n=1}^{n_{\max}} \mathcal{T}_n^{(v)}(\sqrt{B_n(\mu)})$$

for all $v \in M_K^{\mathrm{c}}$. Here $\sigma_v : K \to \mathbb{C}$ is the complex embedding of K associated to v.

In particular, if the intersection is empty for some $v \in M_K^{\mathrm{c}}$, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.

8. An algorithm to bound the canonical height

Combining Proposition 6.2 and Proposition 7.8, we are now ready to state our main theorem.

Theorem 8.1. *Let $\mu > 0$. If $B_n(\mu) < 1$, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. Otherwise, if $B_n(\mu) \geq 1$ for all $n = 1, \ldots, n_{\max}$, then every non-torsion point $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$ satisfies*

$$\varphi_v(\sigma_v(P)) \in \bigcap_{n=1}^{n_{\max}} \mathcal{S}_n^{(v)}(-B_n(\mu), B_n(\mu))$$

for every $v \in M_K^{\mathrm{r}}$, and moreover,

$$\psi_v(\sigma_v(P)) \in \bigcap_{n=1}^{n_{\max}} \mathcal{T}_n^{(v)}(\sqrt{B_n(\mu)})$$

for every $v \in M_K^{\mathrm{c}}$.

In particular, if one of the intersections is empty for some $v \in M_K^{\mathrm{r}} \cup M_K^{\mathrm{c}}$, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.

Theorem 8.1 in turn yields an algorithm for computing a lower bound for the canonical height on $E_{\mathrm{gr}}(K)$, which consists of the following steps:

(1) Given an initial value $\mu > 0$ and the number of steps $n_{\max}$, we start by computing $B_n(\mu)$ for $n = 1, \ldots, n_{\max}$. If $B_n(\mu) < 1$ for some n, then we can conclude immediately that $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.
(2) Otherwise, we proceed to compute $\bigcap_{n=1}^{n_{\max}} \mathcal{S}_n^{(v)}(-B_n(\mu), B_n(\mu))$ for every $v \in M_K^{\mathrm{r}}$. If the intersection is empty for some v, then again $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.
(3) If not, then we compute $\bigcap_{n=1}^{n_{\max}} \mathcal{T}_n^{(v)}(\sqrt{B_n(\mu)})$ for every $v \in M_K^{\mathrm{c}}$. Again, if the intersection is empty for some v, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. Otherwise, we fail to show that μ is a lower bound on $E_{\mathrm{gr}}(K)$.
(4) We can refine μ until sufficient accuracy is achieved, say, if μ is shown to be a lower bound, then we increase μ and repeat the process to see if it is still a lower bound. However, if the algorithm fails to show that μ is a lower bound, then we decrease μ (or increase $n_{\max}$) and repeat the process.
(5) Return the largest value of μ which is known to be a lower bound.

9. Remarks

As in [11], the lower bound we obtain is not model-independent, since, for example, the values α_v in Section 3.2 depend on the coefficients of the Weierstrass model of E. At present, we have not systematically investigated how the bound obtained by our algorithm is affected by a change of model. Note, however, that our formulae can be simplified if E is given by a globally minimal model.

Regarding the computational complexity, it can be seen that computing $B_n(\mu)$ is less time-consuming than computing $\mathcal{S}_n^{(v)}$, which in turn is less time-consuming than computing $\mathcal{T}_n^{(v)}$. Therefore it is plausible to use $B_n(\mu)$ as the first criterion, followed by the intersection of $\mathcal{S}_n^{(v)}$ and $\mathcal{T}_n^{(v)}$, respectively, as we do in our algorithm.

Let c be the least common multiple of all Tamagawa indices as in Section 2. As pointed out by a referee, it may be possible to obtain a larger lower bound by

TABLE 1. Illustration of the algorithm for Example 10.1.

μ	$n_{\max}$	Is any $B_n(\mu) < 1$?	Is any intersection empty?	Is μ a lower bound?
0.20	4	No	No	Fail
0.10	4	No	Yes	Yes
0.15	4	No	Yes	Yes
0.18	4	No	Yes	Yes

making use of the explicit formulae for the local heights at non-archimedean places of bad reduction (see e.g. [9, Theorem 5.2]), provided that c is large. Note that this is different to our approach which uses the subgroup of points of good reduction. In particular, our lower bound on $E(K)$ will be small if c is large. Nonetheless, it might be an interesting area for further study.

10. Examples

We have implemented our algorithm in MAGMA.

Example 10.1. Let E be the elliptic curve over $K = \mathbb{Q}(i)$ given by

$$E: \quad y^2 = x^3 + (91 - 26i)x - (144 + 323i).$$

The discriminant of E can be factorized into a product of prime ideals as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^8$, where

$$\mathfrak{p}_1 = \langle 799 + 1124i \rangle, \quad \mathfrak{p}_2 = \langle 7 - 12i \rangle, \quad \mathfrak{p}_3 = \langle 1 + i \rangle.$$

Hence E is globally minimal. Our algorithm shows that

$$\hat{h}(P) > 0.18$$

for all non-torsion $P \in E_{\mathrm{gr}}(K)$. This is obtained after a number of refinements as shown in Table 1. In this example, we choose $\mathcal{S}^{(v)} = \mathcal{S}^{(v,4)}$ for every $v \in M_K^{\mathrm{c}}$.

The Tamagawa indices of E at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are all 1. Also, $c_v = 1$ where v is the only complex archimedean place of K. Hence $c = 1$, and so

$$\hat{h}(P) > 0.18$$

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

We will now illustrate how to derive a Mordell–Weil basis for $E(K)$ using this lower bound. Here, the torsion subgroup of $E(K)$ is trivial. Let

$$P_1 = (1 + 5i, 2 - i), \quad P_2 = \left(\frac{-32 - 53i}{2}, \frac{-663 + 49i}{4} \right).$$

Then we have $P_1, P_2 \in E(K)$. Moreover, one can check using MAGMA that the rank of $E(K)$ is at most 2. Since

$$R(P_1, P_2) = \det(\langle P_i, P_j \rangle)_{1 \le i,j \le 2} = 3.6050 \neq 0,$$

then P_1 and P_2 are independent. Hence $E(K)$ has rank 2. The geometry of numbers [7, Theorem 3.1] together with the bound just obtained then implies that

$$n = [E(K) : \langle P_1, P_2 \rangle] \le (2\sqrt{3.6050})/(\sqrt{3} \cdot 0.18) = 12.1801.$$

Using a sieving procedure (see [7, Section 4.1]), one can show that n is not divisible by any primes $P \le 11$. Therefore $n = 1$, i.e.,

$$E(K) = \langle P_1, P_2 \rangle.$$

It can be verified that P_1 has the smallest canonical height among non-torsion $P \in E(K)$, with $\hat{h}(P_1) = 1.2326$. Compare this with our lower bound $\hat{h}(P) > 0.18$.

On the other hand, the lower bound obtained by Theorem 5.2 is not as good as the one we just obtained. In this example, we have

$$\alpha_v = 4.715889.$$

We now choose a prime ideal $\mathfrak{p}$ which satisfies $\mathcal{N}(\mathfrak{p}) > \alpha_v$, say, $\mathfrak{p} = \langle 5, 2+i\rangle$. Set $n = e_{\mathfrak{p}} = 5$. Then this yields $D_E(5) = 3.218876$. Finally, we have

$$\hat{h}(P) \geq \mu_0 = (3.218876 - 2\log(4.715889))/(2 \cdot 5^2) = 2.34 \times 10^{-3}.$$

for all non-torsion $P \in E(K)$. If we had used this bound we would only have obtained $n \leq 936$, which would make it harder to check that, in fact, $n = 1$.

Finally, one can verify that the lower bound obtained by [5, Theorem 0.3] is

$$\hat{h}(P) \geq 3.0624 \times 10^{-25}$$

for all non-torsion $P \in E(K)$. We leave it to the reader to compare the results.

Example 10.2. The elliptic curve in this example is from Cremona's paper [3, Example 2]. Let E be the elliptic curve over $K = \mathbb{Q}(i)$ given by

$$E: \quad y^2 + iy = x^3 + (1-i)x^2 - ix.$$

It is verified that $E(K)$ has trivial torsion subgroup, and $P_0 = (0,0) \in E(K)$. In his paper, Cremona asks whether $E(K) = \langle P_0\rangle$. We will show that this is the case.

Let Δ be the discriminant of E. Then we have $\langle\Delta\rangle = \mathfrak{p}$, where $\mathfrak{p} = \langle 13+8i\rangle$. The Tamagawa index at $\mathfrak{p}$ is 1. Again $c_v = 1$ where v is the only complex archimedean place of K. Hence $c = 1$. Using the fact that $\hat{h}(P_0) = 0.0230$, we set our initial guess μ to be smaller than 0.0230, say, $\mu = 0.01$. Our algorithm shows that

$$B_5(\mu) = 0.7772 < 1.$$

Thus by Proposition 5.1, we have $\hat{h}(P) > 0.01$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. Since $c = 1$, we also have $\hat{h}(P) > 0.01$ for all non-torsion $P \in E(K)$.

Using MAGMA, one can check that the rank of $E(K)$ is at most 1. Since P_0 is non-torsion, the rank of $E(K)$ is also at least 1. Hence $E(K)$ has rank 1. Finally, [7, Theorem 3.1] implies that

$$n = [E(K) : \langle P_0\rangle] \leq \sqrt{0.0230/0.01} = 1.5173 < 2,$$

i.e. $n = 1$. Therefore $E(K) = \langle P_0\rangle$.

Example 10.3. Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $x^3 - 2$. Let E be the elliptic curve over K given by

$$E: \quad y^2 = x^3 - (\theta^2 + 3\theta)x + \theta^2.$$

Let Δ be the discriminant of E. Then we have $\langle\Delta\rangle = \mathfrak{p}_1^{16}\mathfrak{p}_2$, where

$$\mathfrak{p}_1 = \langle 2, \theta\rangle, \quad \mathfrak{p}_2 = \langle 390433, 218056 + \theta\rangle.$$

It can be verified that E is globally minimal. Our algorithm shows that

$$\hat{h}(P) > 0.25$$

for all non-torsion $P \in E_{\mathrm{gr}}(K)$. This is obtained after a number of refinements as shown in Table 2. Recall that if $\bigcap \mathcal{S}_n^{(v)} = \emptyset$ for some $v \in M_K^{\mathrm{r}}$, then μ is a lower bound and so there is no need to compute $\bigcap \mathcal{T}_n^{(v)}$ for each $v \in M_K^{\mathrm{c}}$.

TABLE 2. Illustration of the algorithm for Example 10.3.

μ	$n_{\max}$	Is any $B_n(\mu) < 1$?	Is any $\bigcap \mathcal{S}_n^{(v)}$ empty?	Is any $\bigcap \mathcal{T}_n^{(v)}$ empty?	Is μ a lower bound?
0.50	3	No	No	No	Fail
0.20	3	No	Yes	Skipped	Yes
0.30	3	No	No	No	Fail
0.25	3	No	Yes	Skipped	Yes

The Tamagawa indices at $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are 2 and 1, respectively. Moreover, $c_{v_1} = 2$ and $c_{v_2} = 1$ where $v_1 \in M_K^{\mathrm{r}}$ and $v_2 \in M_K^{\mathrm{c}}$. Hence $c = 2$. Thus we finally have

$$\hat{h}(P) > 0.25/2^2 = 0.0625$$

for all non-torsion $P \in E(K)$. Note that in this specific example we have obtained no additional information from the complex place; however, there is no reason to suppose that this would be the case in general.

To derive a Mordell–Weil basis for $E(K)$, first we note that the torsion subgroup of $E(K)$ is trivial. Let

$$P_1 = (0, \theta), \quad P_2 = (1 + \theta, 1), \quad P_3 = (3 - 9\theta + 7\theta^2, 31 + 23\theta - 36\theta^2).$$

Then $P_1, P_2, P_3 \in E(K)$. Moreover, since

$$R(P_1, P_2, P_3) = \det(\langle P_i, P_j \rangle)_{1 \le i,j \le 3} = 0.6263 \neq 0,$$

then P_1, P_2, P_3 are independent. Moreover, one can check using MAGMA that the rank of $E(K)$ is at most 3. Hence $E(K)$ has rank 3. The geometry of numbers [7, Theorem 3.1] together with our lower bound then implies that

$$n = [E(K) : \langle P_1, P_2, P_3 \rangle] \le \sqrt{2(0.6263)}/(\sqrt{0.0625})^3 = 71.6300.$$

Using a sieving procedure (see [7, Section 4.1]), one can actually show that n is not divisible by any primes $p \le 71$. Therefore $n = 1$, i.e.,

$$E(K) = \langle P_1, P_2, P_3 \rangle.$$

It can be verified that P_1 has the smallest canonical height among non-torsion $P \in E(K)$, with $\hat{h}(P_1) = 0.6303$. Compare this with our lower bound $\hat{h}(P) > 0.0625$.

11. Comparison with a searching points method

As suggested by a referee, we finally describe very briefly an alternative way to derive a Mordell–Weil basis as illustrated in [10], and compare it with our method.

Suppose we can find the set $\{P_1, \dots, P_r\} \subset E(K)$ which bijects to a basis for the group $E(K)/mE(K)$ for some $m \ge 2$. Let

$$C_1 = \max\{\hat{h}(Q) : Q = n_1 P_1 + \cdots + n_r P_r, \text{ with } 0 \le n_1, \dots, n_r < m\}.$$

Then [10, Proposition 7.2] says that the set $S = \{R \in E(K) : \hat{h}(R) \le C_1\}$ generates $E(K)$. Using a result of [4] or [10], one can compute a constant C_2 which is an upper bound for $h(P) - \hat{h}(P)$ for all $P \in E(K)$, where $h(P)$ denotes the Weil height of the x-coordinate of P. It then follows that

$$h(R) \le C_1 + C_2$$

for all $R \in S$. This, in principle, will allow one to search for R. If there exist R which are not linear combinations of $P_1, \ldots, P_r$, then we can replace some P_i with linear combinations of such R to obtain a Mordell–Weil basis; otherwise $P_1, \ldots, P_r$ already form such a basis.

The difficulty of this method lies in searching for points. Even though the x-coordinates have bounded height, this can be a non-trivial task especially if $[K : \mathbb{Q}]$ is large. In contrast, our method completely circumvents this problem. If $P_1, \ldots, P_r$ does not yet form a Mordell–Weil basis, we can use a sieving procedure [7, Section 4.1] to derive a new set of candidates. This process, which can be done more quickly than searching for points, however, requires an upper bound for the index $[E(K)/E_{\mathrm{tors}}(K) : \langle P_1, \ldots, P_r \rangle]$, which in turn requires a lower bound for the canonical height.

Acknowledgements

The author wishes to thank his supervisors Dr. Samir Siksek and Professor John E. Cremona for all suggestions during the preparation of this paper. Thanks also go to the Development and Promotion of Science and Technology Talents Project (DPST), Thailand, for its scholarship to his postgraduate study.

References

[1] H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math., vol. 138, Springer-Verlag, 1993. MR1228206 (94i:11105)

[2] J. Cremona and S. Siksek, *Computing a lower bound for the canonical height on elliptic curves over* $\mathbb{Q}$, Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006, Proceedings (F. Hess, S. Pauli, and M. Pohst, eds.), Lecture Notes in Comput. Sci., vol. 4076, Springer-Verlag, 2006, pp. 275–286. MR2282930 (2008d:11066)

[3] J. E. Cremona, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, CRM Proc. Lecture Notes **4** (1994), 29–44. MR1260953 (95i:11046)

[4] J. E. Cremona, M. Prickett, and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), 42–68. MR2197860 (2006k:11121)

[5] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450. MR948108 (89k:11044)

[6] R. E. Moore, *Interval analysis*, Prentice-Hall, Englewood Cliffs, 1966. MR0231516 (37:7069)

[7] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25** (1995), 1501–1538. MR1371352 (97g:11053)

[8] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math., vol. 106, Springer-Verlag, 1986. MR817210 (87g:11070)

[9] ———, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358. MR942161 (89d:11049)

[10] ———, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723–743. MR1035944 (91d:11063)

[11] T. Thongjunthug, *Computing a lower bound for the canonical height on elliptic curves over totally real number fields*, Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17–22, 2008, Proceedings (A. J. van der Poorten and A. Stein, eds.), Lecture Notes in Comput. Sci., vol. 5011, Springer-Verlag, 2008, pp. 139–152. MR2467843

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: T.Thongjunthug@warwick.ac.uk