Computing a Lower Bound for the Canonical Height on Elliptic Curves over Totally Real Number Fields

Thotsaphon Thongjunthug

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
T.Thongjunthug@warwick.ac.uk

Abstract. Computing a lower bound for the canonical height is a crucial step in determining a Mordell–Weil basis of an elliptic curve. This paper presents a new algorithm for computing such lower bound, which can be applied to any elliptic curves over totally real number fields. The algorithm is illustrated via some examples.

1 Introduction

Computing a lower bound for the canonical height is a crucial step in determining a set of generators in Mordell–Weil basis (See [7] for full detail). To be precise, the task of explicit computation of Mordell–Weil basis for $E(K)$, where K is a number field, consists of:

1. A 2-descent (or possibly higher m-descent) is used to determine $P_1, \ldots, P_s$, a basis for $E(K)/2E(K)$ (or $E(K)/mE(K)$ respectively).
2. A lower bound $\lambda > 0$ for the canonical height $\hat{h}(P)$ is determined. This together with the geometry of numbers yields an upper bound on the index n of the subgroup of $E(K)$ spanned by $P_1, \ldots, P_s$.
3. A sieving procedure is used to deduce a Mordell–Weil basis for $E(K)$.

In Step 2, we certainly wish to have the index n as small as possible. In particular, $P_1, \ldots, P_s$ will certainly be a Mordell–Weil basis of $E(K)$ if $n < 2$. It then turns out that, in order to have a *smaller* index, we need to have a *larger* value of the lower bound. This can be seen easily from the following theorem.

Theorem 1. *Let E be an elliptic curve over K. Suppose that $E(K)$ contains no points P of infinite order with $\hat{h}(P) \leq \lambda$ for some $\lambda > 0$. Suppose that $P_1, \ldots, P_s$ generate a sublattice of $E(K)/E_{\mathrm{tors}}(K)$ of full rank $s \geq 1$. Then the index n of the span of $P_1, \ldots, P_s$ in such sublattice satisfies*

$$n \leq R(P_1, \ldots, P_s)^{1/2} (\gamma_s/\lambda)^{s/2} \ ,$$

where $R(P_1, \ldots, P_s) = \det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq s}$ and

$$\langle P_i, P_j \rangle = \frac{1}{2}(\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)) \ .$$

Moreover,

$$\gamma_1^1 = 1, \quad \gamma_2^2 = 4/3, \quad \gamma_3^3 = 2, \quad \gamma_4^4 = 4,$$
$$\gamma_5^5 = 8, \quad \gamma_6^6 = 64/3, \quad \gamma_7^7 = 64, \quad \gamma_8^8 = 2^8,$$

and $\gamma_s = (4/\pi)\Gamma(s/2+1)^{2/s}$ *for* $s \geq 9$.

Proof. See [7, Theorem 3.1]. □

In the past, a number of explicit lower bounds for the canonical height on $E(K)$ has been proposed, including [6, Theorem 0.3]. Although this lower bound has some good properties and is model-independent, it is rather not suitable to computation. For $K = \mathbb{Q}$, there is recently a better lower bound given by Cremona and Siksek [5]. This paper is therefore a generalisation of their work. In particular, we will focus on the case when K is a *totally real* number field.

This work is part of my forthcoming PhD thesis. I wish to thank my supervisor Dr Samir Siksek for all his useful suggestions during the preparation of this paper. I am also indebted to the Development and Promotion of Science and Technology Talent Project (DPST), Ministry of Education of Thailand, for their sponsorship and financial support for my postgraduate study.

1.1 Points of Good Reduction

Suppose K is a totally real number field of degree $r = [K : \mathbb{Q}]$. Let E be an elliptic curve defined over K with discriminant Δ. We define the map

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

with $S = \{\infty_1, \ldots, \infty_r\} \cup \{\mathfrak{p} : \mathfrak{p} \mid \Delta\}$, in such a way that P is mapped into its corresponding point on each real embedding $E^1, \ldots, E^r$ (according as the archimedean places $\infty_1, \ldots, \infty_r$ on K) and its corresponding point on each $E^{(v)}$, a *minimal model* of E at a non-archimedean place v. It is well-known that if K has class number greater than 1, E may not have a *globally minimal* model, i.e. $E^{(v)}$ may differ for different v.

Instead of working directly on $E(K)$, the method we use is to determine a lower bound μ for the canonical height of non-torsion points 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 archimedean v, and the set of points of good reduction for non-archimedean v. In other words, $E_{\mathrm{gr}}(K)$ is the set of points of good reduction on every $E^{(v)}(K_v)$.

Once μ is determined, we can easily deduce the lower bound for the canonical height on the whole $E(K)$: let c be the least common multiple of the Tamagawa indices $c_v = [E^{(v)}(K_v) : E_0^{(v)}(K_v)]$ (including at $v = \infty_1, \ldots, \infty_r$). This is well-defined since $c_v = 1$ for almost all places v. Then the lower bound for the canonical height of all non-torsion points in $E(K)$ is given by $\lambda = \mu/c^2$.

Remark 1. Let v be a non-archimedean place. Suppose E is given by a Weierstrass equation with all coefficients in $\mathcal{O}_v = \{x \in K : \mathrm{ord}_v(x) \geq 0\}$. Let Δ and c_4 be the constants as defined in Section 2. Then E is minimal at v if either $\mathrm{ord}_v(\Delta) < 12$, or $\mathrm{ord}_v(c_4) < 4$.

2 Heights

Throughout this paper, we first define the usual constants of an elliptic curve

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

with $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$, in the following way (See [8, p.46]):

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

Also let

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

so that $x(2P) = g(P)/f(P)$.

In this paper, we use the definition of local and canonical heights as in [4], which is analogous to the one in Cremona's book [3]. This has the same normalisation as the one implemented in MAGMA package, so that both heights can be compared directly. Note that normalisation of heights varies in literature. In particular, our normalisation is twice the one used in Silverman's paper [9].

Denote M_K the set of all places of K. For $P \in E(K)$, define the *naive height* of P by

$$H_K(P) = \prod_{v \in M_K} \max\{1, |x(P)|_v\}^{n_v} \ ,$$

where $n_v = [K_v : \mathbb{Q}_v]$. Observe that

$$H_K(2P) = \prod_{v \in M_K} \max\{|f(P)|_v, |g(P)|_v\}^{n_v} \ .$$

The archimedean places $\infty_1, \infty_2, \ldots, \infty_r$ correspond to the real embeddings $\sigma_1, \sigma_2, \ldots, \sigma_r : K \to \mathbb{R}$, while all non-archimedean places are simply all prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$. For $x \in K$ and $v \in M_K$, the *absolute value* of x at v is given by

$$|x|_v = \begin{cases} |\sigma_j(x)| & \text{if } v = \infty_j \ , \\ \mathcal{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)/n_{\mathfrak{p}}} & \text{if } v = \mathfrak{p}, \text{ a prime ideal} \ , \end{cases}$$

where $\mathcal{N}(\mathfrak{p})$ is the norm of $\mathfrak{p}$. It is verified that this definition satisfies all axioms of valuation theory and the product formula $\prod_{v \in M_K} |x|_v^{n_v} = 1$. From now on, we shall denote $|x|_{\infty_j}$ by $|x|_j$.

The *logarithmic height* of P is then defined by

$$h(P) = \frac{1}{r} \log H_K(P) \ .$$

With these definitions, it can be deduced that

$$h(2P) - 4h(P) = \frac{1}{r} \sum_{v \in M_K} n_v \log \Phi_v(P) \ ,$$

where

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

Using the definition of *canonical height*:

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

and the telescoping sum trick, we have

$$\hat{h}(P) = h(P) + \left[\frac{h(2P)}{4} - h(P)\right] + \left[\frac{h(2^2 P)}{4^2} - \frac{h(2P)}{4}\right] + \ldots = \frac{1}{r} \sum_{v \in M_K} n_v \lambda_v(P) \ ,$$

where

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

Such function $\lambda_v : E(K_v) \to \mathbb{R}$ is called the *local height* at v. This allows us to obtain $\hat{h}(P)$ by combining the contribution of λ_v on each local model $E(K_v)$.

2.1 The Non-Archimedean Local Heights

We shall first consider the properties of λ_v when v is non-archimedean (i.e. $v = \mathfrak{p}$).

For $P \in E(K)$, let $P^{(\mathfrak{p})}$ be its corresponding point (via the map ϕ) on the minimal model $E^{(\mathfrak{p})}$. Let $\lambda_{\mathfrak{p}}$ be the local height associated to E, and $\lambda_{\mathfrak{p}}^{(\mathfrak{p})}$ be the local height associated to $E^{(\mathfrak{p})}$. Assume that E is integral and $E^{(\mathfrak{p})}$ has all coefficients in $\mathcal{O}_{\mathfrak{p}}$, we denote Δ and $\Delta^{(\mathfrak{p})}$ the discriminants of E and $E^{(\mathfrak{p})}$ respectively. These values are related by $\Delta = \left(u^{(\mathfrak{p})}\right)^{12} \Delta^{(\mathfrak{p})}$, for some $u^{(\mathfrak{p})} \in \mathcal{O}_{\mathfrak{p}}$.

The following lemma illustrates the relation between $\lambda_{\mathfrak{p}}$ and $\lambda_{\mathfrak{p}}^{(\mathfrak{p})}$.

Lemma 1.

$$\lambda_{\mathfrak{p}}(P) = \lambda_{\mathfrak{p}}^{(\mathfrak{p})}(P^{(\mathfrak{p})}) + \frac{1}{6} \log |\Delta/\Delta^{(\mathfrak{p})}|_{\mathfrak{p}} \ .$$

Proof. See [4, Lemma 4]. □

Now for $P \in E_{\mathrm{gr}}(K)$, it follows that $P^{(\mathfrak{p})} \in E_0^{(\mathfrak{p})}(K_{\mathfrak{p}})$ at every prime ideal $\mathfrak{p}$. In this case, we can easily compute $\lambda_{\mathfrak{p}}^{(\mathfrak{p})}(P^{(\mathfrak{p})})$ with the following lemma.

Lemma 2. *Let $\mathfrak{p}$ be a prime ideal and $P^{(\mathfrak{p})} \in E_0^{(\mathfrak{p})}(K_{\mathfrak{p}}) \setminus \{O\}$ (i.e. P is a point of good reduction). Then*

$$\lambda_{\mathfrak{p}}^{(\mathfrak{p})}(P^{(\mathfrak{p})}) = \log \max\{1, |x(P^{(\mathfrak{p})})|_{\mathfrak{p}}\} \ .$$

Proof. This is a standard result. See, for example, in [9, Section 5]. □

Note that we may write the principal ideal $\langle x(P^{(\mathfrak{p})})\rangle = AB^{-1}$, where A, B are coprime integral ideals. We call B the *denominator ideal* of $x(P^{(\mathfrak{p})})$, denoted by $\mathrm{denom}(x(P^{(\mathfrak{p})}))$.

The next result is immediate from above lemmas and the definition of $\hat{h}(P)$.

Lemma 3. *Suppose $P \in E_{\mathrm{gr}}(K) \setminus \{O\}$. Then*

$$\hat{h}(P) = \frac{1}{r}\left(\sum_{j=1}^{r} \lambda_{\infty_j}(P) + L(P) - \frac{1}{6}\log \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}\right)\right) \ ,$$

where

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

Proof. From the definition of $\hat{h}(P)$, we have

$$\hat{h}(P) = \frac{1}{r}\sum_{v \in M_K} n_v \lambda_v(P) = \frac{1}{r}\left(\sum_{j=1}^{r} \lambda_{\infty_j}(P) + \sum_{\mathfrak{p}} n_{\mathfrak{p}} \lambda_{\mathfrak{p}}(P)\right) \ , \qquad (2)$$

where (2) follows after we note that

$$n_{\infty_j} = [K_{\infty_j} : \mathbb{Q}_{\infty_j}] = [\mathbb{R} : \mathbb{R}] = 1, \quad \text{for } j = 1, \ldots, r \ .$$

From Lemma 1, we have

$$\begin{aligned}\sum_{\mathfrak{p}} n_{\mathfrak{p}} \lambda_{\mathfrak{p}}(P) &= \sum_{\mathfrak{p}} n_{\mathfrak{p}} \lambda_{\mathfrak{p}}^{(\mathfrak{p})}(P^{(\mathfrak{p})}) + \frac{1}{6}\sum_{\mathfrak{p}} n_{\mathfrak{p}} \log |\Delta/\Delta^{(\mathfrak{p})}|_{\mathfrak{p}} \\ &= \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log \max\{1, |x(P^{(\mathfrak{p})})|_{\mathfrak{p}}\} + \frac{1}{6}\sum_{\mathfrak{p}} n_{\mathfrak{p}} \log |\Delta/\Delta^{(\mathfrak{p})}|_{\mathfrak{p}} \ . \qquad (3)\end{aligned}$$

The last equality follows from Lemma 2, since by assumption $P \in E_{\mathrm{gr}}(K)$ (so that $P^{(\mathfrak{p})} \in E_0^{(\mathfrak{p})}(K_{\mathfrak{p}})$ for all $\mathfrak{p}$). Now recall that

$$|x(P^{(\mathfrak{p})})|_{\mathfrak{p}} = \mathcal{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x(P^{(\mathfrak{p})}))/n_{\mathfrak{p}}} \ .$$

Then for every $\mathfrak{p}$ such that $|x(P^{(\mathfrak{p})})|_{\mathfrak{p}} \leq 1$, the term $\log\{1, |x(P^{(\mathfrak{p})})|_{\mathfrak{p}}\}$ will vanish. Thus all $\mathfrak{p}$ that yield a non-zero value to the first sum in (3) are ones such that $|x(P^{(\mathfrak{p})})|_{\mathfrak{p}} > 1$, i.e. those which divide the denominator ideal of $x(P^{(\mathfrak{p})})$. By definition of absolute value and this fact, the first sum in (3) becomes

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}} \log \max\{1, |x(P^{(\mathfrak{p})})|_{\mathfrak{p}}) = \log \mathcal{N}\left(\prod_{\mathfrak{p}|\mathrm{denom}(x(P^{(\mathfrak{p})}))} \mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(x(P^{(\mathfrak{p})}))} \right) = L(P).$$

Similarly, the second sum in (3) becomes

$$\frac{1}{6} \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log |\Delta/\Delta^{(\mathfrak{p})}|_{\mathfrak{p}} = -\frac{1}{6} \log \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})} \right) \ .$$

Combining these two equalities with (2) yields the result. □

2.2 The Archimedean Local Height Difference

We now consider the archimedean local heights λ_v, i.e. when $v = \infty_1, \ldots, \infty_r$. For $j = 1, \ldots, r$, define

$$\alpha_j^{-3} = \inf_{P \in E_0^j(\mathbb{R})} \Phi_{\infty_j}(P) \ .$$

The exponent -3 is introduced to simplify expressions appearing later. These $\alpha_1, \ldots, \alpha_r$ can be easily computed by method given in [7] with some adjustment.

The following lemma follows directly from the definition of local height.

Lemma 4. *If $P \in E_0^j(\mathbb{R}) \setminus \{O\}$, then*

$$\log \max\{1, |x(P)|_j\} - \lambda_{\infty_j}(P) \leq \log \alpha_j \ .$$

Proof. Rearrange (1) and use the fact that

$$\sum_{i=0}^{\infty} \frac{\log \Phi_{\infty_j}(2^i P)}{4^{i+1}} \geq \sum_{i=0}^{\infty} \frac{\log(\alpha_j^{-3})}{4^{i+1}} = -\log \alpha_j \ .$$

□

3 Multiplication by n

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

Let $k_{\mathfrak{p}}$ be the residue class field of $\mathfrak{p}$, and $e_{\mathfrak{p}}$ 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_p is a finite field, so $c(\mathfrak{p})$ is always a prime number. In particular, $\mathcal{N}(\mathfrak{p}) = |k_{\mathfrak{p}}| \leq c(\mathfrak{p})^r$.

Proposition 1. *If $e_{\mathfrak{p}} \mid n$, then $\mathcal{N}(\mathfrak{p}) \leq (n+1)^{\max\{2,r\}}$. Hence $D_E(n)$ is finite. Moreover, if P is a non-torsion point in $E_{\mathrm{gr}}(K)$ and $n \geq 1$, then*

$$\hat{h}(nP) \geq \frac{1}{r}\left(\sum_{j=1}^{r} \lambda_{\infty_j}(nP) + D_E(n) - \frac{1}{6}\log \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}\right)\right) \ .$$

Proof. Suppose $e_{\mathfrak{p}} \mid n$. If $E^{(\mathfrak{p})}$ has bad reduction at $\mathfrak{p}$, then $e_{\mathfrak{p}}$ is $c(\mathfrak{p})$, $\mathcal{N}(\mathfrak{p})-1$, or $\mathcal{N}(\mathfrak{p})+1$ depending on whether $E^{(\mathfrak{p})}$ has additive, non-split multiplicative, or split multiplicative reduction at $\mathfrak{p}$. In either case, this implies

$$n \geq e_{\mathfrak{p}} \geq \mathcal{N}(\mathfrak{p})^{1/r} - 1 \ ,$$

and thus $\mathcal{N}(\mathfrak{p}) \leq (n+1)^r$. Now for $\mathfrak{p}$ at which $E^{(\mathfrak{p})}$ has good reduction, we have

$$E^{(\mathfrak{p})}_{\mathrm{ns}}(k_{\mathfrak{p}}) = E^{(\mathfrak{p})}(k_{\mathfrak{p}}) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \ ,$$

where $d_1 \mid d_2$ and $d_2 = e_{\mathfrak{p}}$. Hence by Hasse's theorem,

$$(\sqrt{\mathcal{N}(\mathfrak{p})} - 1)^2 \leq |E^{(\mathfrak{p})}_{\mathrm{ns}}(k_{\mathfrak{p}})| = d_1 d_2 \leq e_{\mathfrak{p}}^2 \leq n^2 \ .$$

Thus $\mathcal{N}(\mathfrak{p}) \leq (n+1)^2$. Putting this together yields $\mathcal{N}(\mathfrak{p}) \leq (n+1)^{\max\{2,r\}}$.

The second part follows directly from Lemma 3 once we can show that $L(nP) \geq D_E(n)$. To show this, first note that $P \in E_{\mathrm{gr}}(K)$ implies $P^{(\mathfrak{p})} \in E_0^{(\mathfrak{p})}(K_{\mathfrak{p}})$ for every $\mathfrak{p}$. Define $E_n^{(\mathfrak{p})}(K_{\mathfrak{p}}) = \{P \in E_0^{(\mathfrak{p})}(K_{\mathfrak{p}}) : \mathrm{ord}_{\mathfrak{p}}(x(P)) \leq -2n\}$. Then it is known (see [2, Lemma 7.3.28]) that for all $n \geq 1$,

$$E_n^{(\mathfrak{p})}(K_{\mathfrak{p}})/E_{n+1}^{(\mathfrak{p})}(K_{\mathfrak{p}}) \cong k_{\mathfrak{p}}^{+} \cong (\mathbb{Z}/c(\mathfrak{p})\mathbb{Z})^t \ ,$$

for some $t \in \mathbb{Z}^+$. Let $e(\mathfrak{p}) = \mathrm{ord}_{c(\mathfrak{p})}(n/e_{\mathfrak{p}})$. Then $nP^{(\mathfrak{p})} \in E^{(\mathfrak{p})}_{e(\mathfrak{p})+1}(K_{\mathfrak{p}})$, i.e.

$$\mathrm{ord}_{\mathfrak{p}}(\mathrm{denom}(x(nP^{(\mathfrak{p})}))) \geq 2(e(\mathfrak{p})+1) \ .$$

This implies that $e_{\mathfrak{p}} \mid n$ is equivalent to $\mathfrak{p} \mid \mathrm{denom}(x(nP^{(\mathfrak{p})}))$. Hence

$$\prod_{\mathfrak{p} \mid \mathrm{denom}(x(nP^{(\mathfrak{p})}))} \mathcal{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x(nP^{(\mathfrak{p})}))} \geq \prod_{\substack{\mathfrak{p} \text{ prime} \\ e_{\mathfrak{p}} \mid n}} \mathcal{N}(\mathfrak{p})^{2(e(\mathfrak{p})+1)} \ .$$

Taking logarithm both sides proves our claim. □

4 A Bound for Multiples of Points of Good Reduction

We now wish to show whether a given $\mu > 0$ satisfies $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$. Suppose there exists a non-torsion $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$. Then for each $E^j(\mathbb{R})$ we will obtain a sequence of inequalities satisfied by the x-coordinates of the multiples nP, for $n = 1, \ldots, k$. With suitable μ and k,

the system of inequalities on some $E^j(\mathbb{R})$ may have no solution, which implies $h(P) > \mu$. In this section we will show how to derive such inequalities.

Let α_j and D_E be defined as before. For $\mu > 0$ and $n \in \mathbb{Z}^+$, define

$$B_n(\mu) = \exp\left(rn^2\mu - D_E(n) + \sum_{j=1}^{r} \log \alpha_j + \frac{1}{6} \log \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})} \right) \right) \ .$$

Proposition 2. *If $B_n(\mu) < 1$ then $\hat{h}(P) > \mu$ for all non-torsion points on $E_{\mathrm{gr}}(K)$. On the other hand, if $B_n(\mu) \geq 1$ then for all non-torsion points $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$, we have*

$$|x(nP)|_j \leq B_n(\mu) \ ,$$

for all $j = 1, \ldots, r$.

Proof. Suppose there exists a non-torsion point $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$. From Lemma 4, we have

$$\log \max\{1, |x(nP)|_j\} - \lambda_{\infty_j}(nP) \leq \log \alpha_j \ ,$$

for all $j = 1, \ldots, r$. This implies that

$$\sum_{j=1}^{r} \log \max\{1, |x(nP)|_j\} \leq \sum_{j=1}^{r} \lambda_{\infty_j}(nP) + \sum_{j=1}^{r} \log \alpha_j \ . \tag{4}$$

By Proposition 1 and our assumption that $\hat{h}(P) \leq \mu$, we have

$$\begin{aligned} \sum_{j=1}^{r} \lambda_{\infty_j}(nP) &\leq r\hat{h}(nP) - D_E(n) + \frac{1}{6} \log \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})} \right) \\ &\leq rn^2\mu - D_E(n) + \frac{1}{6} \log \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})} \right) \ . \end{aligned} \tag{5}$$

Combining (4) and (5) and taking exponential, we obtain

$$\prod_{j=1}^{r} \max\{1, |x(nP)|_j\} \leq B_n(\mu) \ .$$

Clearly the left-hand side of this inequality is at least 1. Thus, if $B_n(\mu) < 1$ we simply obtain a contradiction, i.e. $\hat{h}(P) > \mu$ for every non-torsion $P \in E_{\mathrm{gr}}(K)$.

On the other hand, by considering all different cases of $|x(nP)|_j$, it is easy to see that every case implies that $|x(nP)|_j \leq B_n(\mu)$ for all $j = 1, \ldots, r$. □

Corollary 1. *Let $\mathfrak{q}$ be a prime ideal such that*

$$\mathcal{N}(\mathfrak{q}) > \prod_{j=1}^{r} \alpha_j^{1/2} \cdot \mathcal{N}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})} \right)^{1/12} \ , \tag{6}$$

and set $n = e_{\mathfrak{q}}$ *and*

$$\mu_0 = \frac{1}{rn^2}\left(D_E(n) - \sum_{j=1}^{r}\log\alpha_j - \frac{1}{6}\log\mathcal{N}\left(\prod_{\mathfrak{p}}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}\right)\right) \ .$$

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

Proof. Suppose $\mathfrak{q}$ is a prime ideal satisfying (6). By definition of $D_E(n)$, we have

$$D_E(n) \geq 2\log\mathcal{N}(\mathfrak{q}) > \sum_{j=1}^{r}\log\alpha_j + \frac{1}{6}\log\mathcal{N}\left(\prod_{\mathfrak{p}}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}\right) \ ,$$

which implies that $\mu_0 > 0$. Then for any $\mu < \mu_0$, we have

$$\begin{aligned} &rn^2\mu - D_E(n) + \sum_{j=1}^{r}\log\alpha_j + \frac{1}{6}\log\mathcal{N}\left(\prod_{\mathfrak{p}}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}\right) \\ &< rn^2\mu_0 - D_E(n) + \sum_{j=1}^{r}\log\alpha_j + \frac{1}{6}\log\mathcal{N}\left(\prod_{\mathfrak{p}}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\Delta/\Delta^{(\mathfrak{p})})}\right) = 0 \ , \end{aligned}$$

and thus $B_n(\mu) < 1$. Hence $\hat{h}(P) > \mu$ for all non-torsion point $P \in E_{\mathrm{gr}}(K)$ by Proposition 2. Since this is true for all $\mu < \mu_0$, then $\hat{h}(P) \geq \mu_0$ as required. □

It is possible to derive a lower bound for any points on $E_{\mathrm{gr}}(K)$ by Corollary 1 alone. However, our practical experience shows that the bound derived from this corollary itself is not as good as the bound obtained by collecting more information on $x(nP)$. This claim will be illustrated later in our examples.

5 Solving Inequalities Involving the Multiples of Points

From Proposition 2, we know that every non-torsion point $P \in E_{\mathrm{gr}}(K)$ with $\hat{h}(P) \leq \mu$ must satisfy $|x(nP)|_j \leq B_n(\mu)$ for all $j = 1, \ldots, r$. This means that we need to consider r elliptic curves over $\mathbb{R}$, say

$$E^j : \quad y^2 + \sigma_j(a_1)xy + \sigma_j(a_3)y = x^3 + \sigma_j(a_2)x^2 + \sigma_j(a_4)x + \sigma_j(a_6) \ ,$$

for $j = 1, \ldots, r$. In other words, we need to consider $\sigma_j(nP)$ over $E_0^j(\mathbb{R})$. To prove that $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$, we shall derive a contradiction from these inequalities using an application of *elliptic logarithm*.

5.1 Elliptic Logarithm

An elliptic logarithm is an isomorphism $\varphi : E_0(\mathbb{R}) \to \mathbb{R}/\mathbb{Z} \cong [0, 1)$. This can be rapidly computed by method of arithmetic-geometric means. In our program, we use the algorithm in Cohen's book [1, Algorithm 7.4.8] for this computation.

We wish to apply elliptic logarithm to solving our inequalities on these r real embeddings. For $j = 1, \ldots, r$, let

$$\text{On } E^j: \quad f_j(x) = 4x^3 + \sigma_j(b_2)x^2 + 2\sigma_j(b_4)x + \sigma_j(b_6) \ .$$

Note that we can rewrite the Weierstrass equation of E^j as

$$f_j(x) = \left(2y + \sigma_j(a_1)x + \sigma_j(a_3)\right)^2 \ .$$

Denote β_j the largest real root of f_j. On each E^j, we define the corresponding elliptic logarithm φ_j as follows: let

$$\Omega_j = 2\int_{\beta_j}^{\infty} \frac{\mathrm{d}x}{\sqrt{f_j(x)}} \ .$$

Then for a point $P = (\xi, \eta) \in E_0^j(\mathbb{R})$ with $2\eta + \sigma_j(a_1)\xi + \sigma_j(a_3) \geq 0$, we let

$$\varphi_j(P) = \frac{1}{\Omega_j}\int_{\xi}^{\infty} \frac{\mathrm{d}x}{\sqrt{f_j(x)}} \ ,$$

otherwise, let $\varphi_j(P) = 1 - \varphi_j(-P)$.

Suppose that ξ is a real number satisfying $\xi \geq \beta_j$. Then there exists η such that $2\eta + \sigma_j(a_1)\xi + \sigma_j(a_3) \geq 0$ and $(\xi, \eta) \in E_0^j(\mathbb{R})$. Define

$$\psi_j(\xi) = \varphi_j((\xi, \eta)) \in [1/2, 1) \ .$$

In words, $\psi_j(\xi)$ is the elliptic logarithm of the "higher" of the two points on $E_0^j(\mathbb{R})$ with x-coordinate ξ.

For real ξ_1, ξ_2 with $\xi_1 < \xi_2$, we define the subset $\mathcal{S}^j \subset [0, 1)$ as follows:

$$\mathcal{S}^j(\xi_1, \xi_2) = \begin{cases} \emptyset & \text{if } \xi_2 < \beta_j \ , \\ [1 - \psi_j(\xi_2), \psi_j(\xi_2)] & \text{if } \xi_1 < \beta_j \leq \xi_2 \ , \\ [1 - \psi_j(\xi_2), 1 - \psi_j(\xi_1)] \cup [\psi_j(\xi_1), \psi_j(\xi_2)] & \text{if } \xi_1 \geq \beta_j \ . \end{cases}$$

The following lemma is clear.

Lemma 5. *Suppose $\xi_1 < \xi_2$ are real numbers. Then $P \in E_0^j(\mathbb{R})$ satisfies $\xi_1 \leq x(P) \leq \xi_2$ if and only if $\varphi_j(P) \in \mathcal{S}^j(\xi_1, \xi_2)$.*

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

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

Proposition 3. *Suppose $\xi_1 < \xi_2$ are real numbers, and $n > 0$ is an integer. Let*

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

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

Proof. By Lemma 5, $P \in E_0^j(\mathbb{R})$ satisfies $\xi_1 \le x(P) \le \xi_2$ if and only if $\varphi_j(P) \in \mathcal{S}^j(\xi_1, \xi_2)$. Denote the multiplication-by-n map on $\mathbb{R}/\mathbb{Z}$ by ν_n. If $\delta \in [0, 1)$, then

$$\nu_n^{-1}(\delta) = \left\{ \frac{t}{n} + \frac{\delta}{n} : t = 0, 1, 2, \ldots, n-1 \right\} \ .$$

But since φ_j is an isomorphism, we have $\varphi_j(nP) = n\varphi_j(P) \pmod 1$. Hence

$$\varphi_j(nP) \in \mathcal{S}^j(\xi_1, \xi_2) \Longleftrightarrow \varphi_j(P) \in \nu_n^{-1}(\mathcal{S}^j(\xi_1, \xi_2)) = \mathcal{S}_n^j(\xi_1, \xi_2) \ .$$

□

6 The Algorithm

Combining all results we have so far, we obtain our main theorem.

Theorem 2. *Given $\mu > 0$. If $B_n(\mu) < 1$ for some $n \in \mathbb{Z}^+$, then $\hat{h}(P) > \mu$ for every non-torsion point $P \in E_{\mathrm{gr}}(K)$. Otherwise, if $B_n(\mu) \ge 1$ for $n = 1, \ldots, k$, then every non-torsion point $P \in E_{\mathrm{gr}}(K)$ such that $\hat{h}(P) \le \mu$ satisfies*

$$\varphi_j(\sigma_j P) \in \bigcap_{n=1}^{k} \mathcal{S}_n^j(-B_n(\mu), B_n(\mu)) \ ,$$

for all $j = 1, \ldots, r$. In particular, if one of above r intersections is empty, then $\hat{h}(P) > \mu$ for all non-torsion $P \in E_{\mathrm{gr}}(K)$.

To use the algorithm, first we give an initial lower bound μ and the number of steps k. In practice, we find that the initial choice of $\mu = 1$ and $k = 5$ is useful.

We start by computing $B_n(\mu)$ for $n = 1, \ldots, k$. If $B_n(\mu) < 1$ for some n, then we deduce that $\hat{h}(P) > \mu$ for every non-torsion $P \in E_{\mathrm{gr}}(K)$. Otherwise, we compute $\bigcap_{n=1}^{k} \mathcal{S}_n^j(-B_n(\mu), B_n(\mu))$ for $j = 1, \ldots, r$. If the intersection is empty for some j, then again $\hat{h}(P) > \mu$ for every non-torsion $P \in E_{\mathrm{gr}}(K)$. However, if none of r intersections is empty, we fail to show that μ is a lower bound.

We can refine μ further until a sufficient accuracy is achieved: if μ is shown to be a lower bound, we increase μ by some factor, say, 1.1. Otherwise, we decrease μ and increase k, say, by multiplying μ by 0.9 and increasing k by 1. Then we repeat the above with new μ (and possibly new k).

Finally, we return the last value of μ which is known to be a lower bound.

7 Remark

Unlike [6], our lower bound is not model-independent. For example, the values α_j defined in Section 2.2 depend on b_2, b_4, b_6, and b_8. Thus we may obtain different values of lower bound if we work with different models of E. At this point, we are however not to decide which model of E maximises the lower bound. Moreover, our formulae can be simplified if E is a globally minimal model. Note that this may not be the case if E is defined over a field K of class number at least 2.

8 Examples

We have implemented our algorithm in MAGMA to illustrate some examples.

Example 1. Consider the elliptic curve E over $K = \mathbb{Q}(\sqrt{2})$ given by

$$E: \quad y^2 = f(x) = x^3 + x + (1 + 2\sqrt{2}) \ .$$

The discriminant Δ of E is $-3952 - 1728\sqrt{2}$. Moreover, $\langle \Delta \rangle = \mathfrak{p}_1^8 \mathfrak{p}_2^2 \mathfrak{p}_3$, where

$$\mathfrak{p}_1 = \langle \sqrt{2} \rangle, \quad \mathfrak{p}_2 = \langle 7, 3 + \sqrt{2} \rangle, \quad \mathfrak{p}_3 = \langle 769, 636 + \sqrt{2} \rangle \ .$$

Hence by Remark 1, E is minimal at every prime ideal, and thus it is globally minimal. Our program shows that for any non-torsion point $P \in E_{\mathrm{gr}}(K)$,

$$\hat{h}(P) > 0.2415 \ .$$

This is obtained after a number of refinements as shown in Table 1.

Table 1. Illustration of algorithm for Example 1

Initial μ	Initial k	Is any $B_n(\mu) < 1$?	Is any intersection empty?	Is μ a lower bound?	Next μ	Next k
1.0000	5	No	No	Fail	0.5000	6
0.5000	6	No	No	Fail	0.2500	7
0.2500	7	No	No	Fail	0.1250	8
0.1250	8	Yes	Skipped	Yes	0.1875	8
0.1875	8	No	Yes	Yes	0.2187	8
0.2187	8	No	Yes	Yes	0.2343	8
0.2343	8	No	Yes	Yes	0.2421	8
0.2421	8	No	No	Fail	0.2382	9
0.2382	9	No	Yes	Yes	0.2402	9
0.2402	9	No	Yes	Yes	0.2412	9
0.2412	9	No	Yes	Yes	0.2416	9
0.2416	9	No	No	Fail	0.2414	10
0.2414	10	No	Yes	Yes	0.2415	10
0.2415	10	No	No	Fail	0.2415	11
0.2415	11	No	Yes	Yes		

On the other hand, the lower bound for $E_{\mathrm{gr}}(K)$ derived from Corollary 1 is not as good as this one. In this example, we have

$$\alpha_1 = 1.096562, \quad \alpha_2 = 1.001830 \ ,$$

which gives $\alpha_1 \alpha_2 = 1.098569$ We now choose a prime ideal $\mathfrak{p}$ whose norm is greater than $\sqrt{\alpha_1 \alpha_2}$, and set $n = e_{\mathfrak{p}}$. To minimise n, we choose $\mathfrak{p} = \langle \sqrt{2} \rangle$ to get $n = e_{\mathfrak{p}} = 2$. Then we have $D_E(2) = 1.386294$ and finally

$$\mu_0 = (1.386294 - \log(1.098569))/8 = 0.1615 \ .$$

The Tamagawa indices at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are 4, 2, and 1 respectively. Moreover, since $\sigma_1(f)$ and $\sigma_2(f)$ both have one real root, we have $c_{\infty_1} = c_{\infty_2} = 1$. Hence $c = 4$, and thus for any non-torsion point $P \in E(K)$,

$$\hat{h}(P) > 0.2415/16 = 0.0150 \ .$$

It can be checked that the torsion subgroup of $E(K)$ is trivial, and the point $P = (1, 1+\sqrt{2}) \in E(K)$. Using MAGMA, we know that $\hat{h}(P) = 0.5033$, and the rank of $E(K)$ is at most 1. Hence $E(K)$ has rank 1. By Theorem 1, we obtain

$$n = [E(K) : \langle P \rangle] \leq \sqrt{0.5033/0.0150} = 5.7739 \ .$$

Example 2. Consider the elliptic curve E over $K = \mathbb{Q}(\sqrt{7})$ defined by

$$E: \quad y^2 + (3+3\sqrt{7})xy + y = f(x) = x^3 + (26+4\sqrt{7})x^2 + x \ .$$

The discriminant Δ of E is $-937513 - 299394\sqrt{7}$. Moreover, $\langle \Delta \rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where

$$\mathfrak{p}_1 = \langle 4219, 1083+\sqrt{7} \rangle, \quad \mathfrak{p}_2 = \langle 4657, 3544+\sqrt{7} \rangle, \quad \mathfrak{p}_3 = \langle 12799, 5358+\sqrt{7} \rangle \ .$$

Hence by Remark 1, E is minimal at every prime ideal $\mathfrak{p}$, so it is a globally minimal model. Our program shows that for any non-torsion point $P \in E_{\mathrm{gr}}(K)$,

$$\hat{h}(P) > 0.1415 \ .$$

The Tamagawa indices at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are all 1. Also $c_{\infty_1} = c_{\infty_2} = 2$ since both $\sigma_1(f)$ and $\sigma_2(f)$ have 3 real roots. Hence $c = 2$. Then for any non-torsion $P \in E(K)$, we have

$$\hat{h}(P) > 0.1415/4 = 0.0353 \ .$$

In this example, the torsion subgroup of $E(K)$ is trivial. Let $P_1 = (0,0)$ and $P_2 = (1, \sqrt{7})$. It can be verified that both points are on $E(K)$, and

$$\hat{h}(P_1) = 0.8051, \quad \hat{h}(P_2) = 1.4957 \ .$$

Hence by computing the height pairing matrix, we have

$$R(P_1, P_2) = \det \begin{pmatrix} \langle P_1, P_1 \rangle & \langle P_1, P_2 \rangle \\ \langle P_2, P_1 \rangle & \langle P_2, P_2 \rangle \end{pmatrix} = \begin{vmatrix} 0.8051 & -0.1941 \\ -0.1941 & 1.4957 \end{vmatrix} = 1.1665 \neq 0 \ .$$

Therefore P_1 and P_2 are independent. From MAGMA, we know that the rank of $E(K)$ is at most 2. Hence $E(K)$ has rank 2. By Theorem 1, we finally obtain

$$n = [E(K) : \langle P_1, P_2 \rangle] \leq \frac{(\sqrt{1.1665})(2/\sqrt{3})}{0.0353} = 35.2450 \ .$$

Example 3. Let E be the elliptic curve over $K = \mathbb{Q}(\sqrt{10})$ given by

$$E: \quad y^2 = f(x) = x^3 + 125 \ .$$

Note that K has class number 2. By decomposing the discriminant Δ of E, it can be seen that $\langle \Delta \rangle = \langle -2^4 3^3 5^6 \rangle = \mathfrak{p}_1^{12}\mathfrak{p}_2^3\mathfrak{p}_3^3\mathfrak{p}_4^8$, where

$$\mathfrak{p}_1 = \langle 5, \sqrt{10} \rangle, \quad \mathfrak{p}_2 = \langle 3, 4+\sqrt{10} \rangle, \quad \mathfrak{p}_3 = \langle 3, 2+\sqrt{10} \rangle, \quad \mathfrak{p}_4 = \langle 2, \sqrt{10} \rangle \ .$$

By calculating the constant c_4 of E, we have $c_4 = 0$ and so $\mathrm{ord}_{\mathfrak{p}}(c_4) = \infty \not\equiv 4$. Hence by Remark 1, E is minimal everywhere except at $\mathfrak{p}_1$. By substituting

$$x = (\sqrt{10})^2 x', \quad y = (\sqrt{10})^3 y',$$

we have a new elliptic curve $E' : {y'}^2 = {x'}^3 + 1/8$. Now E' is minimal at $\mathfrak{p}_1$ and elsewhere, except at all prime ideals dividing 2. Thus we let $E^{(\mathfrak{p}_1)} = E'$ and $E^{(\mathfrak{p})} = E$ for any $\mathfrak{p} \neq \mathfrak{p}_1$ in our computation. Our program shows that

$$\hat{h}(P) > 0.2859 \ ,$$

for every non-torsion $P \in E_{\mathrm{gr}}(K)$.

The Tamagawa indices at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ are 1, 2, 2, and 1 respectively. Moreover, $\sigma_1(f)$ and $\sigma_2(f)$ both have only one real root, so $c_{\infty_1} = c_{\infty_2} = 1$. Thus $c = 2$, and hence for any non-torsion point $P \in E(K)$, we have

$$\hat{h}(P) > 0.2859/(2^2) = 0.0714 \ .$$

It can be checked that the point $P = (5, 5\sqrt{10}) \in E(K)$. From MAGMA, we know that $\hat{h}(P) = 0.6532$, and the rank of $E(K)$ is at most 1. Hence $E(K)$ must have rank 1. Finally by Theorem 1, we have

$$n = [E(K) : \langle P \rangle] \leq \sqrt{0.6532/0.0714} = 3.0229 \ .$$

References

1. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, 1993.
2. H. Cohen, *Number Theory volume 1: tools and Diophantine equations*, Graduate Texts in Mathematics **239**, Springer, 2007.
3. J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, Cambridge, 1997.
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.
5. J. Cremona and S. Siksek, *Computing a lower bound for the canonical height on elliptic curves over* $\mathbb{Q}$, in Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Lecture Notes in Computer Science **4076**, 275–286, Springer-Verlag, 2006.
6. M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.
7. S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25** (1995), 1501–1538.
8. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, 1986.
9. J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.