

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

Thotsaphon Thongjunthug

Mathematics Institute
University of Warwick

TCC Number Theory Event Day
University of Bristol
21 January 2008

Objectives

- 1 Introduction
 - Elliptic Curves
 - Motivation of Problem

Objectives

1 Introduction

- Elliptic Curves
- Motivation of Problem

2 Methodology

- Main Idea
- Algorithm
- Contribution of Local Heights and Non-Minimality

Objectives

- 1 Introduction
 - Elliptic Curves
 - Motivation of Problem
- 2 Methodology
 - Main Idea
 - Algorithm
 - Contribution of Local Heights and Non-Minimality
- 3 Example

Objectives

- 1 Introduction
 - Elliptic Curves
 - Motivation of Problem
- 2 Methodology
 - Main Idea
 - Algorithm
 - Contribution of Local Heights and Non-Minimality
- 3 Example
- 4 Current Progress

Elliptic Curves

An **elliptic curve** E over a number field K is the set of all (x, y) satisfying the Weierstrass equation

$$E : y^2 = f(x) = x^3 + Ax + B$$

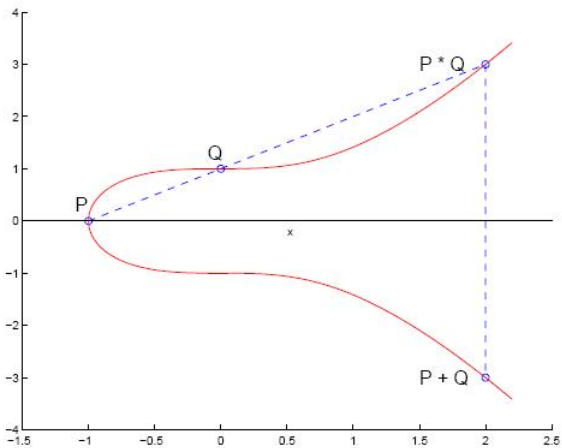
for some $A, B \in K$, with $\Delta = 4A^3 + 27B^2 \neq 0$ (equivalently, $f(x)$ has no repeated roots).

For any field $L \supseteq K$, define the set of **L -points** on E as

$$E(L) = \{(x, y) \in L \times L : y^2 = f(x)\} \cup \{\infty\},$$

where ∞ denotes the **point at infinity**.

The set $E(L)$ is an abelian group under “addition”, with ∞ as the identity.



Moreover,

Theorem (Mordell–Weil)

Let K be a number field. The group $E(K)$ is finitely generated.

Moreover,

Theorem (Mordell–Weil)

Let K be a number field. The group $E(K)$ is finitely generated.

Thus every $P \in E(K)$ is a linear combination of the points

$$T_1, \dots, T_\ell, P_1, \dots, P_s,$$

where

- $T_i \in T =$ **torsion subgroup** (the set of all points having finite order) — easy to compute from Lutz–Nagell theorem.
- P_1, \dots, P_s are independent and have infinite order. The number s is called the **rank** of $E(K)$ — much harder.

Determining a **Mordell–Weil basis** $\{P_1, \dots, P_s\}$ is very important in the study of elliptic curves. This is also related to the concept of **canonical height** of $P \in E(K)$, denoted by $\hat{h}(P)$.

Motivation of Problem

In general, the task of explicit computation of a Mordell–Weil basis consists of:

- 1 A 2-descent is used to determine P_1, \dots, P_s , a basis for $E(K)/2E(K)$.

Motivation of Problem

In general, the task of explicit computation of a Mordell–Weil basis consists of:

- 1 A 2-descent is used to determine P_1, \dots, P_s , a basis for $E(K)/2E(K)$.
- 2 A lower bound $\lambda > 0$ for $\hat{h}(P)$ is somehow determined. This together with the geometry of numbers yields an upper bound for the index $n = [E(K)/T : \langle P_1, \dots, P_s \rangle]$.

Motivation of Problem

In general, the task of explicit computation of a Mordell–Weil basis consists of:

- 1 A 2-descent is used to determine P_1, \dots, P_s , a basis for $E(K)/2E(K)$.
- 2 A lower bound $\lambda > 0$ for $\hat{h}(P)$ is somehow determined. This together with the geometry of numbers yields an upper bound for the index $n = [E(K)/T : \langle P_1, \dots, P_s \rangle]$.
- 3 A sieving procedure is used to deduce a Mordell–Weil basis for $E(K)$.

Motivation of Problem

In general, the task of explicit computation of a Mordell–Weil basis consists of:

- 1 A 2-descent is used to determine P_1, \dots, P_s , a basis for $E(K)/2E(K)$.
- 2 A lower bound $\lambda > 0$ for $\hat{h}(P)$ is somehow determined. This together with the geometry of numbers yields an upper bound for the index $n = [E(K)/T : \langle P_1, \dots, P_s \rangle]$.
- 3 A sieving procedure is used to deduce a Mordell–Weil basis for $E(K)$.

In Step 2, we wish to have n as **small** as possible. By a theorem of Siksek, this can be achieved if we have a **greater** value of λ .

In the past, a number of algorithms to compute a lower bound for $\hat{h}(P)$, where $P \in E(K)$ were proposed. This includes:

- **Hindry and Silverman** (1988): Works for any number field K , but rather theoretically.
- **Cremona and Siksek** (2006): For $K = \mathbb{Q}$ (Recently the sharpest one).

This work is mainly a generalisation of Cremona and Siksek's algorithm. In particular, I aim to extend this algorithm to work for any elliptic curves over **totally real number fields**, and (hopefully) for any number fields at the end.

Main Idea

Suppose K is a totally real number field of degree r . Let E be an elliptic curve over K with discriminant Δ . Define a map

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

where

$$S = \{\infty_1, \dots, \infty_r\} \cup \{\mathfrak{p} \text{ prime ideal in } \mathcal{O}_K : \mathfrak{p} \mid \Delta\},$$

in such a way that each point $P \in E(K)$ is mapped to its corresponding point on each **real embedding** E^1, \dots, E^r , and its corresponding point on $E^{(\mathfrak{p})}$, a **minimal model** of E at \mathfrak{p} .

Each $E^{(\mathfrak{p})}$ may be different if K has class number greater than 1.

We wish to estimate a lower bound for $\hat{h}(P)$, where $P \in E(K)$.
 But instead of working over $E(K)$ itself, we compute a lower bound of $\hat{h}(P)$ for

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

where

$$E_0^{(v)}(K_v) = \begin{cases} \{P \in E(K_v) : P \text{ has good reduction at } v\}, & \text{if } v = \mathfrak{p} \\ \text{“non-loop” component of } E^j(\mathbb{R}), & \text{if } v = \infty_j. \end{cases}$$

In other words, $E_{\text{gr}}(K)$ is the set of all points having **good reduction** on every $E^{(v)}(K_v)$.

Once the lower bound μ for the canonical height on $E_{\text{gr}}(K)$ 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

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

for every place v , including $v = \infty_1, \dots, \infty_r$ (This is well-defined since $c_v = 1$ for almost all v). Then the lower bound for the canonical height of all non-torsion points in $E(K)$ is

$$\lambda = \mu/c^2.$$

Algorithm

To check if $\mu > 0$ is a lower bound for $\hat{h}(P)$ on $E_{\text{gr}}(K)$:

- 1 Start with a given initial guess $\mu > 0$.

Algorithm

To check if $\mu > 0$ is a lower bound for $\hat{h}(P)$ on $E_{\text{gr}}(K)$:

- 1 Start with a given initial guess $\mu > 0$.
- 2 If there exists a non-torsion point $P \in E_{\text{gr}}(K)$ with $\hat{h}(P) \leq \mu$, then this will imply a sequence of inequalities

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

for some function $B_n(\mu)$. This is true for all $v = \infty_1, \dots, \infty_r$.

Algorithm

To check if $\mu > 0$ is a lower bound for $\hat{h}(P)$ on $E_{\text{gr}}(K)$:

- 1 Start with a given initial guess $\mu > 0$.
- 2 If there exists a non-torsion point $P \in E_{\text{gr}}(K)$ with $\hat{h}(P) \leq \mu$, then this will imply a sequence of inequalities

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

for some function $B_n(\mu)$. This is true for all $v = \infty_1, \dots, \infty_r$.

- 3 For a fixed v , combine these inequalities for $n = 1, 2, \dots, k$ for some k .

Algorithm

To check if $\mu > 0$ is a lower bound for $\hat{h}(P)$ on $E_{\text{gr}}(K)$:

- 1 Start with a given initial guess $\mu > 0$.
- 2 If there exists a non-torsion point $P \in E_{\text{gr}}(K)$ with $\hat{h}(P) \leq \mu$, then this will imply a sequence of inequalities

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

for some function $B_n(\mu)$. This is true for all $v = \infty_1, \dots, \infty_r$.

- 3 For a fixed v , combine these inequalities for $n = 1, 2, \dots, k$ for some k .
- 4 With a suitable k , we may see that there is no such P satisfying those inequalities $\implies \hat{h}(P) > \mu$ for all non-torsion $P \in E_{\text{gr}}(K)$.

Algorithm

To check if $\mu > 0$ is a lower bound for $\hat{h}(P)$ on $E_{\text{gr}}(K)$:

- ① Start with a given initial guess $\mu > 0$.
- ② If there exists a non-torsion point $P \in E_{\text{gr}}(K)$ with $\hat{h}(P) \leq \mu$, then this will imply a sequence of inequalities

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

for some function $B_n(\mu)$. This is true for all $v = \infty_1, \dots, \infty_r$.

- ③ For a fixed v , combine these inequalities for $n = 1, 2, \dots, k$ for some k .
- ④ With a suitable k , we may see that there is no such P satisfying those inequalities $\implies \hat{h}(P) > \mu$ for all non-torsion $P \in E_{\text{gr}}(K)$.
- ⑤ Otherwise, we choose a different v and repeat (3)–(5).

Contribution of Local Heights and Non-Minimality

The function $B_n(\mu)$ is indeed given by

$$B_n(\mu) = \exp(rn^2\mu - D_E(n)) \cdot \left(\prod_{j=1}^r \alpha_j \right) \cdot \mathcal{N} \left(\prod_{\mathfrak{p}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(\Delta/\Delta^{(p)})} \right)^{1/6},$$

where

- **Non-archimedean contribution:**

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

Here $c(\mathfrak{p})$ is the characteristic of the residue class field $k_{\mathfrak{p}}$, and $e_{\mathfrak{p}}$ is the exponent of the group $E_{\text{ns}}(k_{\mathfrak{p}})$.

- Archimedean contribution:

$$\alpha_j^{-3} = \inf_{P \in E_0^j(\mathbb{R})} \left\{ \frac{\max\{|f(P)|_{\infty_j}, |g(P)|_{\infty_j}\}}{\max\{1, |x(P)|_{\infty_j}\}^4} \right\},$$

where

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

and $b_2, b_4, b_6, b_8 \in K$ are usual constants associated to E .

- **Archimedean contribution:**

$$\alpha_j^{-3} = \inf_{P \in E_0^j(\mathbb{R})} \left\{ \frac{\max\{|f(P)|_{\infty_j}, |g(P)|_{\infty_j}\}}{\max\{1, |x(P)|_{\infty_j}\}^4} \right\},$$

where

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

and $b_2, b_4, b_6, b_8 \in K$ are usual constants associated to E .

- **Non-minimality contribution:** The term

$$\mathcal{N} \left(\prod_{\mathfrak{p}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(\Delta/\Delta^{(p)})} \right)$$

takes into account when the original model of E over K is non-minimal (either locally or globally).

Example

Let E be the elliptic curve over $K = \mathbb{Q}(\sqrt{2})$ given by

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

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

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

Thus E is already a globally minimal model.

Using the initial $\mu = 1$ and $k = 5$, this algorithm shows that

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

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

The Tamagawa indices at p_1, p_2, p_3 are 4, 2, and 1 respectively. In addition, both real embeddings of E have only one real root, so $c_{\infty_1} = c_{\infty_2} = 1$. Hence $c = \text{lcm}\{4, 2, 1\} = 4$. This gives us

$$\hat{h}(P) > \lambda := 0.2415/4^2 = 0.0150,$$

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

Finally, let $P = (1, 1 + \sqrt{2})$. Then it can be checked that $P \in E(K)$ and P is non-torsion. Assume that $E(K)$ has rank 1, then by Siksek's theorem we have

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

Current Progress

- The algorithm now works for any elliptic curves over totally real number fields.

Current Progress

- The algorithm now works for any elliptic curves over totally real number fields.
- The second phase of this algorithm is to make it works for all elliptic curves over general number fields. Several issues to be concerned include:
 - Extra contribution from complex embeddings. [Known]
 - Solving a sequence of inequalities of $|x(nP)|$, when nP are complex points. [On progress]
 - Computational run-time. [Doubtful]