Computing a Lower Bound for the Canonical Height on Elliptic Curves over $\mathbb{Q}$

John Cremona[1] and Samir Siksek[2]

[1] School of Mathematical Sciences, University of Nottingham
University Park, Nottingham NG7 2RD, UK
John.Cremona@nottingham.ac.uk

[2] Institute of Mathematics, University of Warwick, Coventry, CV4 7AL, UK
siksek@maths.warwick.ac.uk

Abstract. Let E be an elliptic curve over the rationals. A crucial step in determining a Mordell-Weil basis for E is to exhibit some positive lower bound $\lambda > 0$ for the canonical height $\hat{h}$ on non-torsion points.

We give a new method for determining such a lower bound, which does not involve any searching for points.

1 Introduction

Let E be an elliptic curve over the rationals $\mathbb{Q}$ given by a minimal Weierstrass model

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

The task of explicitly computing a Mordell-Weil basis for $E(\mathbb{Q})$ can be divided into three steps (see [10]):

(i) A 2-descent (possibly combined with higher descents) is used to determine a basis $P_1, \ldots, P_r$ for a subgroup of $E(\mathbb{Q})$ of finite index.

(ii) A positive lower bound λ for the canonical height $\hat{\mathrm{h}}(P)$ of non-torsion points is somehow determined. The geometry of numbers now gives an upper bound B on the index n of the subgroup of $E(\mathbb{Q})$ spanned by $P_1, \ldots, P_r$.

(iii) A sieving procedure is finally used to deduce a Mordell-Weil basis.

In step (ii) a rather indirect procedure has been used in the past to determine a lower bound $\lambda > 0$ for the canonical height $\hat{\mathrm{h}}(P)$ of non-torsion points. The difference $\mathrm{h} - \hat{\mathrm{h}}$ between the logarithmic and canonical heights is known to be bounded on $E(\mathbb{Q})$; the best current bounds are to be found in [7]. Suppose that $\mathrm{h}(P) - \hat{\mathrm{h}}(P) \leq K$ for all non-zero rational points P. If $\hat{\mathrm{h}}(P) < \lambda$ then $\mathrm{h}(P) < K + \lambda$. To show that all non-torsion points P satisfy $\hat{\mathrm{h}}(P) \geq \lambda$ one can search for all points satisfying $\mathrm{h}(P) < K + \lambda$. More explicitly, write $x(P) = X/Z^2$ where X, Z are coprime integers and Z positive; then we must search for all points P satisfying

$$|X| < \exp(K + \lambda), \qquad Z < \exp\left((K + \lambda)/2\right).$$

F. Hess, S. Pauli, and M. Pohst (Eds.): ANTS 2006, LNCS 4076, pp. 275–286, 2006.

If the bound on the height difference K is large, then we are forced to search a huge region before achieving our goal; this is quite often impractical.

In this paper we propose a more direct method for determining a positive lower bound λ for the canonical height of non-torsion points.

For reasons to be explained later, it is convenient to work with the subgroup

$$E_{\mathrm{gr}}(\mathbb{Q}) = E(\mathbb{Q}) \cap E_0(\mathbb{R}) \cap \prod_{p \mid \Delta} E_0(\mathbb{Q}_p);$$

the subscript "gr" stands for good reduction, and Δ denotes the minimal discriminant of E, i.e. the discriminant of the minimal model (1). We give a method of determining a positive lower bound μ for the canonical height of non-torsion points P in $E_{\mathrm{gr}}(\mathbb{Q})$. Then, if c is the least common multiple of the Tamagawa indices $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ (including $p = \infty$), we know that $\lambda = \mu/c^2$ is a lower bound for the canonical height of non-torsion points in $E(\mathbb{Q})$.

The basic idea of our approach is very simple: on $E_{\mathrm{gr}}(\mathbb{Q})$, the canonical height satisfies

$$\hat{\mathrm{h}}(P) \geq \log \max \{1, |x(P)|\} - b$$

where b is a constant that depends on the model for E and is typically small. Now if P is 'far from' the the point of order 2 on $E_0(\mathbb{R})$ then its x-coordinate is large and so the canonical height is large. If on the other hand P is 'close to' the point of order 2 on $E_0(\mathbb{R})$ then $x(2P)$ is large, and so $\hat{\mathrm{h}}(P) = \frac{1}{4}\hat{\mathrm{h}}(2P)$ is also large. We extend this idea as follows. Suppose that we want to prove that a certain $\mu > 0$ is a lower bound for the height for non-torsion points on $E_{\mathrm{gr}}(\mathbb{Q})$. We suppose that there is a non-torsion point $P \in E_{\mathrm{gr}}(\mathbb{Q})$ satisfying $\hat{\mathrm{h}}(P) \leq \mu$ and we use this to deduce a series of bounds $|x(nP)| \leq B_n(\mu)$ where the $B_n(\mu)$ are explicit constants. With the aid of the elliptic logarithm, we solve the simultaneous inequalities $|x(nP)| \leq B_n(\mu)$ with $n = 1, \ldots, k$ for some suitably chosen k. If there is no solution then we deduce that $\hat{\mathrm{h}}(P) > \mu$ for all non-torsion points on $E_{\mathrm{gr}}(\mathbb{Q})$. Otherwise we simply start again with a smaller value of μ, or a bigger value of k, or both.

We note that estimates for heights of points of infinite order on elliptic curves have previously been given by Silverman [11] and Hindry and Silverman [8]. Those estimates are theoretical, and too small for practical use; see the concluding remarks at the end of the paper.

2 Heights

In this section we gather some basic facts needed about local and canonical heights, with no claims of originality. A good reference is [13]. The reader is warned that there are several normalizations of local and canonical heights as explained in [7, section 4].

We define the usual constants associated to a Weierstrass model (1) as follows (see [12, page 46]):

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

Let

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

so that $x(2P) = g(P)/f(P)$. We let $\mathcal{M}$ be the set of all primes of $\mathbb{Q}$ (including ∞). For $p \in \mathcal{M}$, define the function $\Phi_p : E(\mathbb{Q}_p) \to \mathbb{R}$ by

$$\Phi_p(P) = \begin{cases} 1 & \text{if } P = 0,\\ \dfrac{\max\{|f(P)|_p, |g(P)|_p\}}{\max\{1, |x(P)|_p\}^4} & \text{otherwise.}\end{cases} \tag{2}$$

It is straightforward to see that Φ_p is a continuous and hence bounded function on $E(\mathbb{Q}_p)$ (the boundedness follows immediately from the fact that $E(\mathbb{Q}_p)$ is compact with respect to the p-adic topology).

We define the local height $\lambda_p : E(\mathbb{Q}_p)\backslash\{0\} \to \mathbb{R}$ for all $p \in \mathcal{M}$ (including $p = \infty$) by

$$\lambda_p(P) = \log\max\{1, |x(P)|_p\} + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_p(2^iP). \tag{3}$$

One definition of the canonical height $\hat{\mathrm{h}} : E(\mathbb{Q}) \to \mathbb{R}$ is by the formula

$$\hat{\mathrm{h}}(P) = \sum_{p\in\mathcal{M}} \lambda_p(P). \tag{4}$$

The canonical height extends to a quadratic form on $\mathbb{R} \otimes_{\mathbb{Z}} E(\mathbb{Q})$; in particular $\hat{\mathrm{h}}(nP) = n^2\,\hat{\mathrm{h}}(P)$ for any integer n. Moreover, $P \in E(\mathbb{Q})$ is torsion if and only if $\hat{\mathrm{h}}(P) = 0$. For non-torsion rational points the canonical height is strictly positive.

The following lemma is standard; see for example [14].

Lemma 1. *Let p be a finite prime and $P \in E_0(\mathbb{Q}_p)\backslash\{0\}$ (i.e. P is a point of good reduction). Then*

$$\lambda_p(P) = \log\max\{1, |x(P)|_p\}.$$

In particular, non-archimedean local heights are non-negative for points of good reduction; this is not true for points of bad reduction. We are interested in obtaining a positive lower bound for the canonical height, using its expression (4) as a sum of local heights, and thus it is sensible to restrict ourselves to points in $E_{\mathrm{gr}}(\mathbb{Q})\backslash\{0\}$.

Our next lemma is immediate from (4) and Lemma 1.

Lemma 2. *Suppose* $P \in E_{\mathrm{gr}}(\mathbb{Q}) \setminus \{0\}$ *. Then*

$$\hat{\mathrm{h}}(P) = \lambda_\infty(P) + \log(\mathrm{denom}(x(P))).$$

2.1 The Archimedean Local Height Difference

Define $\alpha \in \mathbb{R}_+$ by

$$\alpha^{-3} = \inf_{P \in E_0(\mathbb{R})} \Phi_\infty(P), \tag{5}$$

where the exponent -3 has been chosen to simplify the formulae appearing later. This can be computed as in [7] or [10], with a slight adjustment since we are looking only at points on $E_0(\mathbb{R})$. The following lemma can be deduced easily from the definition of local heights (3).

Lemma 3. *If* $P \in E_0(\mathbb{R}) \setminus \{0\}$ *then*

$$\log \max\{1, |x(P)|\} - \lambda_\infty(P) \le \log \alpha.$$

In particular this inequality is true for all $P \in E_{\mathrm{gr}}(\mathbb{Q}) \setminus \{0\}$*.*

3 Multiplication by n

Let n be a positive integer. It is possible that multiplication by n annihilates some of the groups $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$: a non-torsion point $P \in E_{\mathrm{gr}}(\mathbb{Q})$ will be killed (mapped into $E_1(\mathbb{Q}_p)$) if p divides the denominator of $x(nP)$. In this section we give a lower estimate for the contribution that multiplication by n makes to the canonical height of nP.

For finite primes p, let e_p be the exponent of the group

$$E_{\mathrm{ns}}(\mathbb{F}_p) \cong E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p).$$

Define

$$D_E(n) = \sum_{p < \infty,\, e_p \mid n} 2(1 + \mathrm{ord}_p(n/e_p)) \log p. \tag{6}$$

That this sum is finite follows from the following proposition; clearly, it is easily computable.

Proposition 1. *With notation as above, if* $e_p \mid n$ *then* $p \le (n+1)^2$*. Hence the sum defining* $D_E(n)$ *is finite. Moreover, if* P *is a non-torsion point in* $E_{\mathrm{gr}}(\mathbb{Q})$ *and* $n \ge 1$*, then*

$$\hat{\mathrm{h}}(nP) \ge \lambda_\infty(nP) + D_E(n).$$

Proof. Suppose that $e_p \mid n$. By definition e_p is the exponent of $E_{\mathrm{ns}}(\mathbb{F}_p)$. If p is a prime of singular reduction for E then $E_{\mathrm{ns}}(\mathbb{F}_p)$ is a cyclic group of order

$p-1$, $p+1$ or p depending on whether E has split multiplicative, non-split multiplicative or additive reduction at p. In either case we see that

$$n \geq e_p = |E_{\mathrm{ns}}(\mathbb{F}_p)| \geq p-1$$

and so certainly $p \leq (n+1)^2$. Suppose now that p is a prime of good reduction. We know that

$$E_{\mathrm{ns}}(\mathbb{F}_p) = E(\mathbb{F}_p) \cong \mathbb{Z}/d_1 \times \mathbb{Z}/d_2$$

where $d_2|d_1$ and $d_1 = e_p$. Hence

$$(\sqrt{p}-1)^2 = p+1-2\sqrt{p} \leq |E(\mathbb{F}_p)| = d_1 d_2 \leq d_1^2 = e_p^2 \leq n^2,$$

from which we deduce that $p \leq (n+1)^2$.

In view of Lemma 2, the proof is complete on showing

$$\log(\mathrm{denom}(x(nP))) \geq D_E(n)$$

for non-torsion $P \in E_{\mathrm{gr}}(\mathbb{Q})$. This easily follows from the structure of $E(\mathbb{Q}_p)$, since if $e = \mathrm{ord}_p(n/e_p)$ then $nP \in E_{e+1}(\mathbb{Q}_p)$, so $\mathrm{ord}_p(\mathrm{denom}(x(nP))) \geq 2(e+1)$. □

4 A Bound for Multiples of Points of Good Reduction

Recall that our aim is to exhibit some positive μ such that $\hat{\mathrm{h}}(P) > \mu$ for all non-torsion points in $E_{\mathrm{gr}}(\mathbb{Q})$. In this section we first suppose that $\mu > 0$ is given, assume that P is a point in $E_{\mathrm{gr}}(\mathbb{Q})$ satisfying $\hat{\mathrm{h}}(P) \leq \mu$, and deduce a sequence of inequalities satisfied by the x-coordinates of the multiples nP for $n = 1, 2, 3, \ldots$. We then show that for sufficiently small positive μ and a suitable n (given explicitly in Corollary 1 below), there are no points P such that $x(nP)$ satisfies the inequality. In the following two sections we will explain how to combine the inequalities for several n, enabling us to obtain better values of μ such that $\hat{\mathrm{h}}(P) > \mu$ for non-torsion points in $E_{\mathrm{gr}}(\mathbb{Q})$.

Let α and D_E be defined as above in (5) and (6). For $\mu > 0$ and $n \in \mathbb{Z}^+$ define

$$B_n(\mu) = \exp\left(n^2\mu - D_E(n) + \log\alpha\right).$$

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

$$-B_n(\mu) \leq x(nP) \leq B_n(\mu).$$

Proof. Suppose P is a non-torsion point on $E_{\mathrm{gr}}(\mathbb{Q})$ with $\hat{\mathrm{h}}(P) \leq \mu$. From the inequalities in Lemma 3 and Proposition 1 we see that

$$\begin{aligned}\log\max\{1, |x(P)|\} &\leq \lambda_\infty(P) + \log\alpha \\ &\leq \hat{\mathrm{h}}(nP) - D_E(n) + \log\alpha \\ &= n^2\,\hat{\mathrm{h}}(P) - D_E(n) + \log\alpha \\ &\leq n^2\mu - D_E(n) + \log\alpha.\end{aligned}$$

Thus

$$\max\{1, |x(nP)|\} \leq B_n(\mu).$$

If $B_n(\mu) < 1$ then we have a contradiction, and in this case we deduce that $\hat{\mathrm{h}}(P) > \mu$ for all non-torsion points on $E_{\mathrm{gr}}(\mathbb{Q})$.

If instead $B_n(\mu) \geq 1$, then $|x(nP)| \leq B_n(\mu)$ and the proposition follows. □

Corollary 1. *Define α as in (5). Let p be a prime greater than $\sqrt{\alpha}$, and set $n = e_p$ and $\mu_0 = n^{-2}(D_E(n) - \log \alpha)$. Then $\mu_0 > 0$ and for all non-torsion $P \in E_{\mathrm{gr}}(\mathbb{Q})$ we have*

$$\hat{\mathrm{h}}(P) \geq \mu_0.$$

Proof. We have $D_E(n) \geq 2 \log p > \log \alpha$, so certainly $\mu_0 > 0$. Now for all $\mu < \mu_0$ we have $n^2\mu - D_E(n) + \log \alpha < 0$, so that $B_n(\mu) < 1$ and hence $\hat{\mathrm{h}}(P) > \mu$ by the Proposition. Since this holds for all $\mu < \mu_0$, we have $\hat{\mathrm{h}}(P) \geq \mu_0$ as required.

As pointed out to us by the anonymous referee, we could use this Corollary by itself to provide a suitable positive lower bound for the height of non-torsion points in $E_{\mathrm{gr}}(\mathbb{Q})$. However we can obtain a better bound (see Example 1 for an example) by combining the information from several different n simultaneously.

5 Solving Inequalities Involving the Multiples of Points

Proposition 2 gives a sequence of inequalities involving the multiples of non-torsion points P in $E_{\mathrm{gr}}(\mathbb{Q})$ satisfying $\hat{\mathrm{h}}(P) \leq \mu$. We would like to solve these inequalities. One approach is to use division polynomials. We have found this impractical as the degree and coefficients of division polynomials grow rapidly with the multiple considered. Instead we have found it convenient to use the elliptic logarithm.

For the reader's convenience, we give here a very brief description of the elliptic logarithm $\varphi : E_0(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}$. We can rewrite the Weierstrass model (1) as

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Let β be the largest real root of the right-hand side; thus β is the x-coordinate of the unique point of order 2 on $E_0(\mathbb{R})$. Let

$$\Omega = 2\int_{\beta}^{\infty} \frac{\mathrm{d}x}{\sqrt{4x^3 + b_2x^2 + 2b_4x + b_6}}.$$

If $P = (\xi, \eta) \in E_0(\mathbb{R})$ with $2\eta + a_1\xi + a_3 \geq 0$ then let

$$\varphi(P) = \frac{1}{\Omega}\int_{\xi}^{\infty} \frac{\mathrm{d}x}{\sqrt{4x^3 + b_2x^2 + 2b_4x + b_6}};$$

otherwise we let

$$\varphi(P) = 1 - \varphi(-P).$$

The elliptic logarithm can be very rapidly computed using arithmetic-geometric means; see Algorithm 7.4.8 in [2]. What matters most to us is that $\varphi : E_0(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}$ is an isomorphism (of real Lie groups). We shall find it convenient to identify $\mathbb{R}/\mathbb{Z}$ with the interval $[0,1)$.

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

$$\psi(\xi) = \varphi\left((\xi,\eta)\right) \in [1/2, 1).$$

In words, $\psi(\xi)$ is the elliptic logarithm of the "higher" of the two points with x-coordinate ξ.

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

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

The following lemma is clear.

Lemma 4. *Suppose $\xi_1 < \xi_2$ are real numbers. Then $P \in E_0(\mathbb{R})$ satisfies $\xi_1 \leq x(P) \leq \xi_2$ if and only if $\varphi(P) \in \mathcal{S}(\xi_1,\xi_2)$.*

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

$$t + \bigcup [a_i, b_i] = \bigcup [a_i + t, b_i + t]$$

and (for $t > 0$)

$$t \bigcup [a_i, b_i] = \bigcup [ta_i, tb_i].$$

Proposition 3. *Suppose $\xi_1 < \xi_2$ are real numbers and n a positive integer. Define*

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

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

Proof. By Lemma 4 we know that $P \in E_0(\mathbb{R})$ satisfies $\xi_1 \leq x(nP) \leq \xi_2$ if and only if $\varphi(nP) \in \mathcal{S}(\xi_1,\xi_2)$.

Denote the multiplication by n map on $\mathbb{R}/\mathbb{Z}$ by ν_n. If $\delta \in [0,1)$ then

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

However $\varphi(nP) = n\varphi(P) \pmod 1$. Therefore,

$$\varphi(nP) \in \mathcal{S}(\xi_1,\xi_2) \iff \varphi(P) \in \nu_n^{-1}\left(\mathcal{S}(\xi_1,\xi_2)\right) = \mathcal{S}_n(\xi_1,\xi_2).$$

□

6 The Algorithm

Putting together Propositions 2 and 3 we deduce our main result.

Theorem 1. *Let $\mu > 0$. If $B_n(\mu) < 1$ for some positive integral n, then $\hat{\mathrm{h}}(P) > \mu$ for all non-torsion P in $E_{\mathrm{gr}}(\mathbb{Q})$.*

On the other hand, if $B_n(\mu) \geq 1$ for $n = 1, \ldots, k$, then every non-torsion point $P \in E_{\mathrm{gr}}(\mathbb{Q})$ such that $\hat{\mathrm{h}}(P) \leq \mu$ satisfies

$$\varphi(P) \in \bigcap_{n=1}^{k} \mathcal{S}_n\left(-B_n(\mu), B_n(\mu)\right).$$

In particular, if

$$\bigcap_{n=1}^{k} \mathcal{S}_n\left(-B_n(\mu), B_n(\mu)\right) = \emptyset \tag{7}$$

then $\hat{\mathrm{h}}(P) > \mu$ for all non-torsion P in $E_{\mathrm{gr}}(\mathbb{Q})$.

In practice we have found the following procedure effective. We start with $\mu = 1$, $k = 5$ and compute $B_n(\mu)$ for $n = 1, \ldots k$. If any of these values of $B_n(\mu) < 1$ then we have succeeded in proving that $\mu = 1$ is a lower bound for the canonical height of non-torsion points of good reduction. Otherwise we compute $\bigcap_{n=1}^{k} \mathcal{S}_n\left(-B_n(\mu), B_n(\mu)\right)$ (as a union of intervals); if this is empty, then again we have succeeded in proving that $\mu = 1$ is a lower bound. Finally, if this intersection is non-empty we have failed to prove that $\mu = 1$ is a suitable lower bound.

Our course now proceeds differently according to whether we have succeeded or failed to show that $\mu = 1$ is a lower bound. If we succeed, we now repeatedly multiply μ by 1.1 and use the same method to try to prove that the new value of μ is still a lower bound. We return the last succeeding value of μ as the output to the algorithm.

If, on the other hand, we failed with $\mu = 1$ then we repeatedly multiply μ by 0.9 and increase k by 1 until we achieve success; the bound returned is then the first successful value of μ.

It is easy to use the proof of Corollary 1 to Proposition 2 to show that our algorithm will succeed in obtaining a positive lower bound μ, after a finite number of steps.

Alternative strategies are clearly possible here; instead of using scaling factors of 11/10 and 9/10 we could instead use a larger factor such as 2 or 1/2 respectively, and then successively replace the scaling factor by its square root and apply a back-tracking method to converge to the optimal value of μ; the details may be left to the reader.

7 Reduced Models

The canonical height is independent of the model chosen for the elliptic curve. Our lower bound is however not model-independent. The constant α defined in (5) is dependent on b_2, b_4, b_6; all other constants and maps in the above discussion are model-independent. To improve our lower bound for the canonical height it is sensible to choose a model that minimises the value of α. We have no theoretical method for deciding on the best model here. The models for elliptic curves appearing in Cremona's tables [3], [5] (as well as those appearing in the earlier Antwerp IV tables [1]) are known as standardized models: we say that the model (1) for E is a standardized model if it is minimal with $a_1, a_3 \in \{0, 1\}$, and $a_2 \in \{-1, 0, 1\}$. Each elliptic curve has a unique standardized model. Practical experience shows that—for the purpose of obtaining a good lower bound for the canonical height—it is usually preferable to choose a model that reduces, in the sense of [4] but with respect to translations only, the cubic polynomial

$$f(X) = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

We call this model the reduced model. For the convenience of the reader we give here the formulae, adapted from [4], for doing this.

If the discriminant $\varDelta > 0$, then we let

$$P = b_2^2 - 24b_4, \qquad Q = 2b_2b_4 - 36b_6.$$

Let r be the nearest integer to $-Q/(2P)$. The reduced model for E is given by replacing x by $x + r$ in (1).

If $\varDelta < 0$ we let β be the unique real root of f. Let

$$h_0 = 36\beta^2 + 24b_2\beta + 48b_4 - b_2^2, \quad h_1 = 24b_2\beta^2 + 6(b_2^2 - 8b_4)\beta + 4b_2b_4.$$

Let r be the nearest integer to $-h_1/(2h_0)$. Again, the reduced model for E is given by replacing x by $x + r$ in (1).

8 Examples

We have implemented our algorithm in `pari/gp`, and used the program to compute some examples.

Example 1. Consider the elliptic curve E (with code 60490d1 in [5]), given by the standardized model

$$y^2 + xy + y = x^3 + 421152067x + 105484554028056.$$

Our program shows that for non-torsion points in $E_{\mathrm{gr}}(\mathbb{Q})$

$$\hat{\mathrm{h}}(P) > 1.9865.$$

If we apply the method used to prove Corollary 1 to Proposition 2 above, we do not obtain as good a bound. Here $\log(\alpha) = 3.3177\ldots$ and $\sqrt{\alpha} = 5.253\ldots$, so we should use a prime $p \geq 7$. Rather than use $p = 7$ for which $e_p = 9$ we do better to take $p = 19$ with $n = e_p = 6$. Then $D_E(6) = 2\log 114$ and $\mu_0 = (2\log 114 - 3.317)/36 = 0.17$.

We note that the curve E has only one real component. Moreover, it has good reduction at all primes except 2, 5, 23 and 263 where the Tamagawa indices are 2, 21, 2 and 3 respectively. Hence if $P \in E(\mathbb{Q})$ then $42P \in E_{\mathrm{gr}}(\mathbb{Q})$. It follows that

$$\hat{\mathrm{h}}(P) > 1.9865/42^2 = 0.001126$$

for non-torsion points in $E(\mathbb{Q})$.

This curve has rank 1, and a point of infinite order is

$$P = (3583035/169, 24435909174/2197)$$

with $\hat{\mathrm{h}}(P) = 6.808233192$. It follows that the index of the subgroup $\langle P\rangle$ in $E(\mathbb{Q})$ is at most $\sqrt{6.808233192/0.001126} < 78$. We may check that $P \notin pE(\mathbb{Q})$ for all primes $p < 78$ (using the method of p-saturation introduced in [10]) and deduce that $E(\mathbb{Q}) = \langle P\rangle$.

For this curve the bound between logarithmic and canonical heights can be shown by the method of [7] to be at most 22.8, so finding a lower bound for $\hat{\mathrm{h}}$ through searching would be prohibitive. However, if we apply the method of [7] to the subgroup $E_{\mathrm{gr}}(\mathbb{Q})$ we find that the height difference for points in the subgroup is only 3.3, so in fact we could have found a lower bound for the restriction of $\hat{\mathrm{h}}$ to the subgroup by searching for points with small logarithmic height.

Finally, we can use our bound to prove that $E(\mathbb{Q}) = \langle P\rangle$ more simply as follows. First we apply p-saturation with $p = 2$, 3 and 7 to show that the index $[E(\mathbb{Q}) : \langle P\rangle]$ is not divisible by the primes dividing the Tamagawa numbers; then we observe that while $P \notin E_{\mathrm{gr}}(\mathbb{Q})$, we have $2P \in E_{\mathrm{gr}}(\mathbb{Q})$. It follows that $[E(\mathbb{Q}) : E_{\mathrm{gr}}(\mathbb{Q})] = 2$, when *a priori* this index could have been as large as 42. And moreover the index $m = [E(\mathbb{Q}) : \langle P\rangle] = [E_{\mathrm{gr}}(\mathbb{Q}) : \langle 2P\rangle]$ is coprime to $2, 3, 7$ and satisfies $m^2 \leq \hat{\mathrm{h}}(2P)/1.9865 < 14$, so $m = 1$.

This method of saturating $E(\mathbb{Q})$, by first saturating $E_{\mathrm{gr}}(\mathbb{Q})$ and separately saturating at primes dividing the Tamagawa numbers, can also be used for curves of higher rank, though the details are more complicated. We will return to this in a future paper.

Example 2. (Statistics) We ran our program on all the 4081 optimal curves in our online tables [5] with conductors 7000–8000. The smallest lower bound we obtained for that range was 0.022 for curve 7042d1, and the largest was 11.879 for 7950r1. It took 941 seconds to compute the lower bounds for these curves, an average of 0.23 seconds for each curve.

Applications. Using this method we intend to show that the generators listed for the curves in the database [5] do generate the full Mordell-Weil group, modulo torsion, in every case. The present situation (January 2006) is that not all have been checked, the exceptions being those for which we have not yet obtained a lower bound for the height of non-torsion points, and hence do not have a bound in the index of saturation. Similarly, the algorithm described here will be incorporated into the first author's program mwrank (see [6]) for computing Mordell-Weil groups via 2-descent.

9 Concluding Remarks

As pointed out by the referee, it would be possible to extend this method to elliptic curves defined over any totally real number field; we leave the details to the interested reader. It would be rather harder, though, to extend our method to fields with a non-real complex embedding since we would then have to intersect subsets of the unit square instead of the unit interval.

Lastly, at the insistence of the referee, we conclude with a few words comparing our lower bound for the canonical height and earlier theoretical bounds, due to Silverman [11] and to Hindry and Silverman [8]. The bounds of [11] are not completely explicit. In [8], Hindry and Silverman give a lower bound for the canonical height of non-torsion points on elliptic curves over number fields (and function fields). For example, if E is an elliptic curve over $\mathbb{Q}$, write

$$\sigma = \frac{\log|\Delta|}{\log N}$$

where Δ is the minimal discriminant and N is the conductor of E. Specializing Theorem 0.3 of [8] we obtain that

$$\hat{\mathrm{h}}(P) \geq \frac{2\log|\Delta|}{(20\sigma)^8 10^{1.1+4\sigma}}.$$

for non-torsion points $P \in E(\mathbb{Q})$. For example, for the elliptic curve E in our Example 1, this gives the lower bound for non-torsion points

$$\hat{\mathrm{h}}(P) \geq 3.2\ldots \times 10^{-42},$$

as compared with our lower bound for non-torsion points $\hat{\mathrm{h}}(P) > 0.001126$. However such a crude numerical comparison is not very useful, for two reasons:

- The bounds in [8] are much more general; undoubtedly the methods there could produce better bounds if specialised to elliptic curves over the rationals. It would be interesting to pursue this.
- A conjecture of Lang (mentioned in [8]) states that there is some absolute constant $c > 0$ such that $\hat{\mathrm{h}}(P) \geq c\log|\Delta|$ for all elliptic curves E and non-torsion points $P \in E(\mathbb{Q})$. The objective of [8] seems to have been to prove a statement that is as close as possible to Lang's conjecture. Our aim is rather different.

References

1. B.J. Birch and W. Kuyk (eds.), *Modular Functions of One Variable IV*, Lecture Notes in Mathematics **476**, Springer-Verlag, 1975.
2. H. Cohen, *A Course in Computational Algebraic Number Theory (Third Corrected Printing).* Graduate Texts in Mathematics **138**, Springer-Verlag, 1996.

3. J.E. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, 1996.
4. J.E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 62–92.
5. J.E. Cremona, *Elliptic Curve Data*, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`.
6. J.E. Cremona, `mwrank`, a program for computing Mordell-Weil groups of elliptic curves over $\mathbb{Q}$. Available from `http://www.maths.nott.ac.uk/personal/jec/mwrank`.
7. J.E. Cremona, M. Prickett and S. Siksek, *Height difference bounds for elliptic curves over number fields*, Journal of Number Theory **116** (2006), 42–68.
8. M. Hindry and J. H. Silverman, *The Canonical Height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.
9. PARI/GP, version `2.2.8`, Bordeaux, 2004; available from `http://pari.math.u-bordeaux.fr/`.
10. S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain Journal of Mathematics **25**, number 4 (Fall 1995), 1501–1538.
11. J.H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Mathematical Journal **48** (1981), 633–648.
12. J.H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.
13. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, 1994.
14. J.H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339-358.