Elements with bounded height in number fields

A. Pethő*, S Schmitt

November 28, 2009

Dedicated to Professor András Sárközy on the occasion of his 60th birthday.

Abstract. We give a constructive proof of the fact that there exist only finitely many elements with bounded height in number fields. This provides an efficient method to enumerate all those elements. Such a method is helpful to compute bases on elliptic curves.

Mathematics subject classification numbers, 11R33, 11G50, 14G05.

Key words and phrases, Algebraic number fields, integral bases, LLL-reduction, absolute height, elliptic curves, Néron-Tate height, Mordell-Weil basis of elliptic curves.

1 Introduction

Let $\mathbb{K}$ be a number field of degree $n = [\mathbb{K} : \mathbb{Q}] = s + 2t$, where s denotes the number of real and $2t$ the number of complex isomorphisms of $\mathbb{K}$. Let $M_{\mathbb{K}}$ be the set of inequivalent absolute values in $\mathbb{K}$. For an absolute value v let n_v be the local degree. The absolute height of the element $x \in \mathbb{K}$ is defined by

$$H(x) = \left(\prod_{v \in M_{\mathbb{K}}} \max\{1, |x|_v\}^{n_v} \right)^{1/n}.$$

This measure is very convenient for theoretical purposes. It is well known (see e.g. J. Silverman [8]) that for any $A \in \mathbb{R}, A \geq 1$, there exist only finitely many $x \in \mathbb{K}$ with $H(x) \leq A$.

In this article we fix a positive number $A \in \mathbb{R}, A \geq 1$, and consider the set

$$S_A := \{x \in \mathbb{K} \ : \ H(x) \leq A\}.$$

Using Manin's conditional algorithm [4] (for details see S. Schmitt [6]) to compute a basis of an elliptic curve over $\mathbb{K}$ one gets a maximal set of linearly independent points on the curve. The basis can then be computed using an

[*] Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T25157 and T16975

index estimate of S. Siksek [7]. For this estimate one has to check for a fixed A all elements $x \in S_A$ whether there exists $y \in \mathbb{K}$ such that the point (x, y) is lying on the curve. A similar problem arises in the 2-descent algorithm, where one has to test equations of the form $y^2 = g(x)$, where $g(x)$ is a quartic polynomial, whether they have a solution (x, y) in $\mathbb{K}^2$ (cf e.g. [2], [9]). To solve such problems one has to provide an efficient method to enumerate all elements of bounded height.

In Section 3 we use the method of searching points of bounded height developed in the preceding sections to compute bases on elliptic curves over quadratic number fields.

In the case $\mathbb{K} = \mathbb{Q}$ every $x \in \mathbb{Q}$ can be written as $x = a/b$, with integers a, b such that $b > 0$ and $\gcd(a, b) = 1$. For elements of number fields we have an analogous representation. For every $x \in \mathbb{K}$ there exist an algebraic integer $\alpha \in \mathbb{Z}_\mathbb{K}$ and a positive rational integer c such that $x = \alpha/c$. Choosing an integral basis $\omega_1, \ldots, \omega_n$ of $\mathbb{Z}_\mathbb{K}$ the element $x \in \mathbb{K}$ can be written as

$$x = \frac{a_1\omega_1 + \cdots + a_n\omega_n}{c}$$

with $a_1, \ldots, a_n, c \in \mathbb{Z}$. These parameters are obviously not at all unique. For $x \in S_A$ the size of $a_1, \ldots, a_n$, and c depends not only on A, but also on the choice of the integral basis.

For $x \in \mathbb{K}$ denote by $x^{(k)}$ the conjugates of x, $1 \leq k \leq n$. Adapting the notation of M. Pohst [5] let

$$T_2(x) = \sum_{k=1}^{n} |x^{(k)}|^2$$

for $x \in \mathbb{K}$.

Theorem 1. *Let $A \in \mathbb{R}, A \geq 1$. Further, let $\Omega = \{\omega_1, \ldots, \omega_n\}$ be an integral basis of $\mathbb{Z}_\mathbb{K}$ and $D_\mathbb{K}$ the discriminant of $\mathbb{K}$. Then any $x \in S_A$ can be represented in the form*

$$x = \frac{a_1\omega_1 + \ldots + a_n\omega_n}{c}$$

with $a_1, \ldots, a_n, c \in \mathbb{Z}$, satisfying

$$0 < c \leq A^n$$

and

$$|a_i| \leq \frac{A^n c\sqrt{n}}{|D_\mathbb{K}|^{1/2}} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} T_2(\omega_j)^{1/2} =: B_i(\mathbb{K}, \Omega, A, c)$$

for $i = 1, \ldots, n$.

In the present note we also prove that it is possible to choose the integral basis $\omega_1, \ldots, \omega_n$ such that for $x \in S_A$ the bound for the size of $a_1, \ldots, a_n$ and c depends only on A and $\mathbb{K}$. From the proof of Theorem 3 it will be clear that

$\omega_1, \dots, \omega_n$ can be computed from an arbitrary integral basis by using the very efficient LLL algorithm discovered by A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász [3]. More precisely we prove the following theorem.

Theorem 2. *Let $A \in \mathbb{R}, A \geq 1$. Denote by $2t$ the number of non-real isomorphisms of $\mathbb{K}$. There exists an integral basis $\omega_1, \dots, \omega_n$ of $\mathbb{Z}_{\mathbb{K}}$ such that any $x \in S_A$ can be represented in the form $a_1, \dots, a_n, c \in \mathbb{Z}$ with the properties*

$$x = \frac{a_1\omega_1 + \dots + a_n\omega_n}{c}$$

with $a_1, \dots, a_n, c \in \mathbb{Z}$ satisfying

$$0 < c \leq A^n$$

and

$$|a_i| \leq 2^{n(n+1)/4-t} A^n c =: B_i(\mathbb{K}, A, c)$$

for $i = 1, \dots, n$.

2 Proofs of Theorem 1 and Theorem 2

For the proof of the theorems we need some auxiliary results. To state them we fix some notation.

Denote by $M_{\mathbb{K},0}$ the set of discrete valuations of $\mathbb{K}$. For a prime ideal $\mathfrak{p}$ let $v_{\mathfrak{p}} \in M_{\mathbb{K},0}$ be the non-archimedian absolute value corresponding to $\mathfrak{p}$ and $n_{\mathfrak{p}} = n_{v_{\mathfrak{p}}}$ the corresponding local degree. The normalized additive absolute value is then $\mathrm{ord}_{v_{\mathfrak{p}}}(x)$ with

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

For simplicity in the sequel we write $\mathrm{ord}_{\mathfrak{p}}(x)$ instead of $\mathrm{ord}_{v_{\mathfrak{p}}}(x)$.

Lemma 1. *Let $x \in \mathbb{K}$ such that $H(x) \leq A$. Then there exist $\alpha \in \mathbb{Z}_{\mathbb{K}}$ and $c \in \mathbb{Z}$ such that $x = \frac{\alpha}{c}$ and $0 < c \leq A^n$.*

Proof. By the unique prime ideal decomposition theorem we can write the fractional ideal (x) in the form

$$(x) = \mathfrak{q}_1\mathfrak{q}_2^{-1},$$

where

$$\mathfrak{q}_1 = \prod_{\substack{\mathfrak{p} \in M_{\mathbb{K},0} \\ \mathrm{ord}_{\mathfrak{p}}(x) > 0}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x)} \quad \text{and} \quad \mathfrak{q}_2 = \prod_{\substack{\mathfrak{p} \in M_{\mathbb{K},0} \\ \mathrm{ord}_{\mathfrak{p}}(x) < 0}} \mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(x)}.$$

Then $\mathfrak{q}_2$ is an integral ideal. Denote its norm by c. Then c is a positive integer and the principal ideal (c) is divisible by $\mathfrak{q}_2$. There exists an integral ideal $\mathfrak{q}_3$ such that $(c) = \mathfrak{q}_2\mathfrak{q}_3$. Hence

$$(x) = \mathfrak{q}_1\mathfrak{q}_3(c)^{-1},$$

which implies that $\mathfrak{q}_1\mathfrak{q}_3$ is a principal ideal, too. Denoting its generator by β we obtain

$$(x) = (\beta)(c)^{-1},$$

which proves the first assertion of the lemma by taking $\alpha = \beta\varepsilon$ for a suitable unit ε.

Now we estimate the size of c. We have

$$c = \mathcal{N}(\mathfrak{q}_2) = \prod_{\substack{\mathfrak{p}\in M_{\mathbb{K},0} \\ \mathrm{ord}_{\mathfrak{p}}(x)<0}} \mathcal{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)} = \prod_{\substack{\mathfrak{p}\in M_{\mathbb{K},0} \\ \mathrm{ord}_{\mathfrak{p}}(x)<0}} |x|_{v_{\mathfrak{p}}}^{n_{\mathfrak{p}}} \leq H(x)^n.$$

The lemma is proved. □

Proof of Theorem 1. If $H(x) \leq A$ then by Lemma 1 there exist an algebraic integer $\alpha \in \mathbb{Z}_{\mathbb{K}}$ and a rational integer $c \in \mathbb{Z}, c > 0$ such that $x = \alpha/c$ and $c \leq A^n$. The assumption $H(x) \leq A$ implies that for all $v \in M_{\mathbb{K}}$

$$|x|_v \leq A^{n/n_v} \leq A^n,$$

hence

$$|\alpha|_v \leq A^n |c|_v.$$

If we consider archimedian absolute values, we see that for all conjugates of α

$$|\alpha^{(k)}| \leq A^n c.$$

Choose an integral basis $\omega_1, \ldots, \omega_n$ of $\mathbb{Z}_{\mathbb{K}}$. Then α can be written in the form

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n$$

with $a_i \in \mathbb{Z}$. Taking conjugates and using Cramer's rule we see that

$$a_i = \frac{D_i}{D_{\mathbb{K}}^{1/2}},$$

where

$$D_i = \det \begin{pmatrix} \omega_1^{(1)} & \ldots & \alpha^{(1)} & \ldots & \omega_n^{(1)} \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \omega_1^{(n)} & \ldots & \alpha^{(n)} & \ldots & \omega_n^{(n)} \end{pmatrix}$$

is the determinant of the matrix $(\omega_j^{(k)})_{1\leq j,k\leq n}$, where the i-th column is replaced by the vector $(\alpha^{(k)})_{1\leq k\leq n}$.

By means of the Hadamard inequality for D_i the estimate

$$\begin{aligned} |D_i| &\leq \left(\sum_{k=1}^n |\alpha^{(k)}|^2\right)^{1/2} \prod_{\substack{1\leq j\leq n \\ j\neq i}} \left(\sum_{k=1}^n |\omega_j^{(k)}|^2\right)^{1/2} \\ &= \left(\sum_{k=1}^n |\alpha^{(k)}|^2\right)^{1/2} \prod_{\substack{1\leq j\leq n \\ j\neq i}} T_2(\omega_j)^{1/2} \end{aligned}$$

holds. The inequality

$$\sum_{k=1}^{n} |\alpha^{(k)}|^2 \leq \sum_{k=1}^{n} A^{2n}c^2 = A^{2n}c^2 n$$

proves the theorem. □

Recall that the number field $\mathbb{K}$ has s real and $2t$ non-real embeddings into the field of complex numbers. Order the conjugate fields as usual so that $\mathbb{K}^{(1)}, \ldots, \mathbb{K}^{(s)}$ denote the real and $\mathbb{K}^{(s+1)}, \ldots, \mathbb{K}^{(s+t)}$, $\overline{\mathbb{K}^{(s+1)}}, \ldots, \overline{\mathbb{K}^{(s+t)}}$ denote the non-real conjugate fields of $\mathbb{K}$.

M. Pohst [5] proved that there exists a $\mathbb{Q}$-basis $\rho_1 = 1, \rho_2, \ldots, \rho_n$ of algebraic integers in $\mathbb{K}$ such that

$$\prod_{i=1}^{n} T_2(\rho_i) \leq \gamma_n^n |D_{\mathbb{K}}|,$$

where γ_n^n denotes the Minkowski constant. Unfortunately $\rho_1 = 1, \rho_2, \ldots, \rho_n$ is usually not an integral basis, hence this result is not applicable in our situation. Using ideas of J. Buchmann and A. Pethő [1] we are able to prove the existence of an integral basis such that the product of the T_2-norm of the basis elements is small. Moreover the proof gives us an algorithm for the computation of such a basis.

Theorem 3. *Let $\mathbb{K}$ be of degree $n = s + 2t$ and with discriminant $D_{\mathbb{K}}$. There exists an integral basis $\omega_1, \ldots, \omega_n$ in $\mathbb{K}$ such that*

$$\prod_{i=1}^{n} T_2(\omega_i) \leq 2^{n(n+1)/2-2t} |D_{\mathbb{K}}|.$$

Proof. ¿From the geometry of numbers it is well known that the mapping

$$\begin{array}{rcl} \phi : \mathbb{K} & \rightarrow & \mathbb{R}^n \\ x & \mapsto & \underline{x} = (x^{(1)}, \ldots, x^{(s)}, \Re x^{(s+1)}, \ldots, \Re x^{(s+t)}, \Im x^{(s+1)}, \ldots, \Im x^{(s+t)})^T \end{array}$$

is a morphism of $\mathbb{K}$ and the image $\phi(\mathbb{Z}_{\mathbb{K}})$ is a complete lattice in $\mathbb{R}^n$. We have further

$$\det(\phi(\mathbb{Z}_{\mathbb{K}}))^2 = 2^{-2t}|D_{\mathbb{K}}|.$$

The application of the LLL algorithm [3] to the lattice $\phi(\mathbb{Z}_{\mathbb{K}})$ leads to an integral basis $\omega_1, \ldots, \omega_n$ with

$$\prod_{i=1}^{n} |\underline{\omega}_i| \leq 2^{n(n-1)/4} \det(\phi(\mathbb{Z}_{\mathbb{K}})) = 2^{n(n-1)/4-t} |D_{\mathbb{K}}|^{1/2},$$

where $|\underline{\omega}_i|^2 = \sum\limits_{j=1}^{s+t} |\omega_i^{(j)}|^2$. Since

$$T_2(\omega_i) = \sum_{j=1}^{n} |\omega_i^{(j)}|^2 \leq 2|\underline{\omega}_i|^2$$

we may conclude

$$\prod_{i=1}^{n} T_2(\omega_i) \leq 2^n \prod_{i=1}^{n} |\underline{\omega}_i|^2 \leq 2^{n(n+1)/2-2t}|D_{\mathbb{K}}|.$$

Theorem 3 is proved. □

We are now in the position to prove Theorem 2.

Proof of Theorem 2. If $H(x) \leq A$ then by Theorem 1 there exist integers $b_1, \ldots, b_n, c \in \mathbb{Z}, c > 0$ such that

$$\begin{array}{rcl} \alpha & = & b_1\omega_1' + \ldots + b_n\omega_n' \\ x & = & \dfrac{\alpha}{c} \\ 0 & < & c \leq A^n \end{array}$$

and

$$|b_i| \leq \frac{A^n c\sqrt{n}}{|D_{\mathbb{K}}|^{1/2}} \prod_{\substack{1\leq j\leq n \\ j\neq i}} T_2(\omega_j')^{1/2},$$

where $\omega_1', \ldots, \omega_n'$ is an arbitrary integral basis of $\mathbb{Z}_{\mathbb{K}}$. Now choose an integral basis $\omega_1, \ldots, \omega_n$ of $\mathbb{Z}_{\mathbb{K}}$, which existence was proved in Theorem 2 and write α in the form

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n.$$

As the ω_i's are non-zero algebraic integers the absolute values of their norms are at least 1. The inequality between the arithmetic and geometric mean implies

$$T_2(\omega_i) \geq n, \quad i = 1, \ldots, n.$$

Therefore

$$\prod_{\substack{1\leq j\leq n \\ j\neq i}} T_2(\omega_j)^{1/2} \leq \frac{1}{\sqrt{n}} \prod_{1\leq j\leq n} T_2(\omega_j)^{1/2}.$$

By Theorem 3 we obtain

$$\prod_{1\leq j\leq n} T_2(\omega_j) \leq 2^{n(n+1)/2-2t}|D_{\mathbb{K}}|.$$

Hence for $i = 1, \ldots, n$

$$|a_i| \leq \frac{A^n c\sqrt{n}}{|D_{\mathbb{K}}|^{1/2}} \cdot \frac{1}{\sqrt{n}} \cdot 2^{n(n+1)/4-t}|D_{\mathbb{K}}|^{1/2} = 2^{n(n+1)/4-t}A^n c$$

as required. The theorem is proved. □

3 Examples

The computations in this section were performed using the computer algebra system SIMATH (see [10]).

In their article [2], J. Cremona and P. Serf use descent methods to compute the rank of elliptic curves over real quadratic number fields with class number one. They give 8 examples of elliptic curves, where they also find a maximal set of linearly independent points.

We now compute a basis for those elliptic curves from the examples which have rank > 0. Therefore we estimate the index of the group generated by the points found in [2]. Such an estimate is given in the following theorem of S. Siksek.

Theorem 4. *Let E be an elliptic curve of rank $r > 0$ over the number field $\mathbb{K}$. Let*

$$0 < \lambda \leq \inf\{\hat{h}(P) : P \in E(\mathbb{K}) \backslash E(\mathbb{K})_{tors}\}$$

be an estimate for the minimal Néron–Tate height of non torsion points. Further let $P_1, \ldots, P_r$ be linearly independent points on $E(\mathbb{K})$. Then the index n of the subgroup generated by $P_1, \ldots, P_r$ in $E(\mathbb{K})$ satisfies

$$n \leq R_{P_1,\ldots,P_r}^{1/2} \left(\frac{\gamma_r}{\lambda}\right)^{r/2}.$$

Here $R_{P_1,\ldots,P_r}$ is the regulator of the points $P_1, \ldots, P_r$ and γ_r^r are the Minkowski constants, i.e.

$$\begin{array}{llll} \gamma_1^1 = 1, & \gamma_2^2 = \frac{4}{3}, & \gamma_3^3 = 2, & \gamma_4^4 = 4, \\ \gamma_5^5 = 8, & \gamma_6^6 = \frac{64}{3}, & \gamma_7^7 = 64, & \gamma_8^8 = 2^8 \end{array}$$

and for $r \geq 9$ one has

$$\gamma_r = \frac{4}{\pi} \Gamma\left(\frac{r}{2} + 1\right)^{2/r}.$$

Proof. See the article of Siksek [7]. □

To use this theorem we have to compute an estimate for the minimal Néron-Tate height of non torsion points. This is done in the following way. Choose $\varepsilon > 0$ and find all points in the set

$$T_\varepsilon := \{P \in E(\mathbb{K}) \backslash E(\mathbb{K})_{\text{tors}} : \hat{h}(P) < \varepsilon\}.$$

Then take

$$\lambda := \begin{cases} \min\{\hat{h}(P) : P \in T_\varepsilon\} & \text{if } T_\varepsilon \neq \emptyset \\ \varepsilon & \text{if } T_\varepsilon = \emptyset. \end{cases}$$

For computing the set T_ε we need the difference between the Néron-Tate height and the Weil height on elliptic curves

$$h(P) - \hat{h}(P) \leq \delta \quad \text{for a } \delta \in \mathbb{R}, \delta \geq 0.$$

In his article [7], Siksek also gives an algorithm to compute an estimate for δ. We compute this estimate for the examples. Then we find the points

$$\{P \in E(\mathbb{K}) : h(P) < \varepsilon + \delta\}.$$

This is the same as finding all elements in

$$S_A := \{x \in \mathbb{K} : H(x) < \exp(\varepsilon + \delta) =: A\}.$$

For every element of S_A we test if it corresponds to a point on E and if this point is in the set T_ε. Then we get the estimate λ.

Each element of the quadratic number field is denoted by an ordered pair of integers which are its coefficients with respect to the standard integral basis. The curves are defined as $E = [a_1, a_2, a_3, a_4, a_6]$ where the a_i are the coefficients of the Weierstraß normal form. We only consider those elliptic curves from [2] where the rank is > 0.

Example 1: $\mathbb{K} = \mathbb{Q}(\sqrt{5}), E = [(2,0), (-2,0), (-1,-1), (0,1), (0,-1)]$
Rank: $r = \mathrm{rk}(E(\mathbb{K})) = 2$
Linearly independent points found in [2]:

Point	Néron-Tate height
$P_1 = ((0,0),(1,0))$	0.2117441002
$P_2 = ((8,-5),(-33,21))$	1.2698716559

Regulator: $R_{P_1,P_2} = 0.0807304562$

δ	ε	A	λ	index
0	0.2	1.2214027582	0.2	≤ 1.6404314085

We find no point with Néron-Tate height $\leq \varepsilon$, hence we can take $\lambda = 0.2$. As the index of the group generated by P_1, P_2 is < 2, these points form a basis of $E(\mathbb{K})$.

Example 2: $\mathbb{K} = \mathbb{Q}(\sqrt{5}), E = [(-2,0), (-2,-1), (2,-2), (-2,1), (0,0)]$
Rank: $r = \mathrm{rk}(E(\mathbb{K})) = 3$
Linearly independent points found in [2]:

Point	Néron-Tate height
$P_1 = (1/4(-2,3), 1/8(3,4))$	2.0288667203
$P_2 = ((-1,1),(-4,3))$	0.3580740908
$P_3 = ((37,-23),(-228,141))$	1.8363230414

Regulator: $R_{P_1,P_2,P_3} = 0.1057930442$

δ	ε	A	λ	index
0.4497421983	0.4	2.3390437647	0.3580740908	≤ 2.1467635270

We find two points with Néron-Tate height $\leq \varepsilon$: $\pm P_2$.

The results in the article [2] are computed using 2-descent. Therefore the index of the group generated by the given points is not divisible by 2. From this fact and the estimate for the index we see that P_1, P_2, P_3 form a basis of $E(\mathbb{K})$.

Example 3: $\mathbb{K} = \mathbb{Q}(\sqrt{2}), E = [(0,0),(2,1),(0,0),(1,0),(-1,-1)]$
Rank: $r = \mathrm{rk}(E(\mathbb{K})) = 1$
Linearly independent points found in [2]:

Point	Néron-Tate height
$P_1 = ((0,-1),(1,-1))$	0.6661477648

Regulator: $R_{P_1} = 0.6661477648$

δ	ε	A	λ	index
0.5333320118	0.6	3.1059884677	0.0740164183	≤ 3.0000000002

We find four points with Néron-Tate height $\leq \varepsilon$:

Point	Néron-Tate height
$Q_1 = ((1,1),(-3,-2))$	0.2960656732
$-Q_1 = ((1,1),(3,2))$	0.2960656732
$Q_2 = ((-1,-1),(-1,0))$	0.0740164183
$-Q_2 = ((-1,-1),(1,0))$	0.0740164183

¿From the estimate for the index and the fact that the index has to be odd, we see that we have to test if the index is divisible by 3. It is easy to check that

$$3Q_2 = P_1 \quad \text{and} \quad (-2)Q_2 = Q_1,$$

so the index of the group generated by P_1 in $E(\mathbb{K})$ is equal to 3. A basis of $E(\mathbb{K})$ is given by Q_2.

Example 4: $\mathbb{K} = \mathbb{Q}(\sqrt{13}), E = [(0,2),(0,-1),(1,2),(0,1),(0,1)]$
Rank: $r = \mathrm{rk}(E(\mathbb{K})) = 1$
Linearly independent points found in [2]:

Point	Néron-Tate height
$P_1 = (1/4(-3,0),1/8(-3,-2))$	2.1920662705

Regulator: $R_{P_1} = 2.1920662705$

δ	ε	A	λ	index
0.2090249966	0.3	1.6636683217	0.0876826508	≤ 5.0000000006

We find two points with Néron-Tate height $\leq \varepsilon$:

Point	Néron-Tate height
$Q_1 = ((-1,1),(-2,1))$	0.0876826508
$-Q_1 = ((-1,1),(-5,-3))$	0.0876826508

¿From the estimate for the index we see that we have to test if the index is divisible by 3 and by 5. It is easy to check that

$$5Q_1 = P_1,$$

so the index is divisible by 5 and we get the basis Q_1 of $E(\mathbb{K})$.

Example 5: $\mathbb{K} = \mathbb{Q}(\sqrt{3}), E = [(2,2),(1,1),(0,0),(0,2),(-2,-2)]$
Rank: $r = \mathrm{rk}(E(\mathbb{K})) = 2$
Linearly independent points found in [2]:

Point	Néron-Tate height
$P_1 = ((-2,-1),(10,5))$	1.2626912790
$P_2 = (1/121(1756,-1405), 1/1331(169325,-77612))$	5.1558657383

Regulator: $R_{P_1,P_2} = 1.3558456945$

δ	ε	A	λ	index
0.0486645137	1	2.8538373114	1	≤ 1.3445423977

We find no point with Néron-Tate height $\leq \varepsilon$, hence we can take $\lambda = 1$. As the index of the group generated by P_1, P_2 is < 2, these points form a basis of $E(\mathbb{K})$.

In the examples we have not found any points with Néron-Tate height equal to 0. Hence we have proven that these curves have no torsion points.

Acknowledgment. We are grateful to D. Simon and J. Cremona for their interesting comments with regard to this paper, especially for pointing out some simplifications in the examples.

References

[1] J. Buchmann and A. Pethő, *Computation of Independent Units in Number Fields by Dirichlet's Method,* Math. Comput. **52** (1989), 149-159 and S1-S14.

[2] J. Cremona and P. Serf, *Computing the rank of elliptic curves over real quadratic number fields of class number 1*, Math. Comput. **68** (1999), 1187-1200.

[3] A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515-534.

[4] Yu.I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), 7-78.

[5] M. Pohst, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory, **14** (1982), 99–117.

[6] S. Schmitt, *Bestimmung der Mordell-Weil Gruppe elliptischer Kurven über algebraischen Zahlkörpern.* Thesis, Univ. des Saarlandes, 1999.

[7] S. Siksek, *Infinite Descent on Elliptic Curves*, Rocky Mountain J. Math. **25** (1995), 1501-1538.

[8] J. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Math., Vol. **106**, Springer Verlag, Berlin 1986.

[9] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math., to appear.

[10] SIMATH, *A computer algebra system for algorithmic number theory*, http://simath.math.uni-sb.de.

A. Pethő
Institute of Mathematics and Informatics
University of Debrecen
P.O. Box 12
4010 Debrecen
Hungary
email: pethoe@math.klte.hu

S. Schmitt
FB Mathematik
Universität des Saarlandes
Postfach 151150
66041 Saarbrücken
Germany
email: susanne@math.uni-sb.de