MATHEMATICS OF COMPUTATION
Volume 78, Number 266, April 2009, Pages 1201–1210
S 0025-5718(08)02160-1
Article electronically published on July 1, 2008

# PARALLEL LLL-REDUCTION FOR BOUNDING THE INTEGRAL SOLUTIONS OF ELLIPTIC DIOPHANTINE EQUATIONS

L. HAJDU AND T. KOVÁCS

Abstract. Stroeker and Tzanakis gave convincing numerical and heuristic evidence for the fact that in their $\mathcal{E}llog$ method a certain parameter $\lambda$ plays a decisive role in the size of the final bound for the integral points on elliptic curves. Furthermore, they provided an algorithm to determine the Mordell-Weil basis of the curve which corresponds to the optimal choice of $\lambda$. In this paper we show that working with more Mordell-Weil bases simultaneously, the final bound for the integral points can be further decreased.

## 1. Introduction

Elliptic Diophantine equations have a long history. Even the effective theory of such equations has an extremely rich literature. A classical result of Baker [1] yields that an elliptic equation can have only finitely many integer solutions, and the size (absolute value) of the solutions can be effectively bounded. Later, this result was extended and improved by several authors; see e.g. [16], [14], [13], [12], [22], [3], [8], [4] and the references given there. For related results see also the book [15] and the references therein.

However, to explicitly find all integral solutions another method has been developed, which uses the arithmetic properties of elliptic curves. This algorithm combines many deep ingredients, due to several authors. Here we only refer to the papers of Stroeker, Tzanakis [17] and Gebel, Pethő, and Zimmer [6], where the first complete versions of this method are independently given. (See also the references in these papers.) Later, the method of Stroeker and Tzanakis, the so-called $\mathcal{E}llog$ method was developed further. The most recent version is already capable of finding (at least in principle) all integral points on genus one curves (see [19], and also the references given there for certain important intermediate steps). To summarize the method in one sentence, what happens is that first the maximum $N$ of the coefficients of the integral points (in some Mordell-Weil basis) is bounded, and then this bound is gradually decreased to a size where the actual points can now be identified by an exhaustive search. (Of course, in fact, the method is much more general and complicated.) To get the final bound $N_{final}$ for $N$, the LLL-algorithm is applied. In [18], Stroeker and Tzanakis observed and gave convincing numerical and heuristic evidence for the fact that in getting $N_{final}$, a certain parameter $\lambda$

Received by the editor December 18, 2007 and, in revised form, March 12, 2008.
2000 *Mathematics Subject Classification.* Primary 11G05, Secondary 11Y50.
*Key words and phrases.* Elliptic curves, integral points, LLL-reduction.
Research supported in part by the Hungarian Academy of Sciences and by the OTKA grants T48791 and K67580.

plays a decisive role. In fact, this $\lambda$ is the smallest eigenvalue of the height pairing matrix of the underlying Mordell-Weil basis. Furthermore, they provided an algorithm for determining a Mordell-Weil basis which corresponds to the optimal choice of $\lambda$. Hence to minimize the final bound for the solutions, one should use such a "best" basis of the curve. We shall call such a basis a Stroeker-Tzanakis basis, or shortly an ST-basis. In [18] it is shown through several examples that using an ST-basis one can get a (much) better bound $N_{final}$ than with other bases. This point is important, in particular, if the rank of the elliptic curve is "large", since then a small improvement of the final bound can considerably shrink the region of possible solutions, and hence the final search can be done much faster.

The purpose of this paper is to show that even the "best" final bound $N_{final}$ received by using an ST-basis, can be further improved if one uses more bases simultaneously, and combines the information obtained for the solutions in the different bases. As we will also see, elementary linear algebra tells us that it takes only very little extra time to get this improvement.

In the next section, in order to present our method, first we need to (schematically) outline the main steps of the $\mathcal{E}llog$ method, with particular emphasize on the parameter $\lambda$. Then we explain our method, as well. In the third section we give some examples to illustrate how our method works.

Finally, we mention that in the case of $S$-unit equations one faces an analogous situation. There the fundamental systems of $S$-units play a similar role to the Mordell-Weil bases. Furthermore, it turns out that there a particular parameter also plays a decisive role in the size of the reduced bound for the solutions, and it is possible to define and construct a "best" system of fundamental $S$-units with respect to this parameter (see [7]). Furthermore, the final bound obtained by using any (even the "best") system, can be developed by using more systems of fundamental $S$-units simultaneously (cf. [9]). We do not go into details here.

## 2. Bounding integral solutions of genus one equations

In this section we first briefly summarize the main steps of the $\mathcal{E}llog$ method of Stroeker and Tzanakis. We follow the presentation in [19] without any further reference.

Let $f \in \mathbb{Z}[u, v]$ and define the curve $C$ by

$$C: \quad f(u, v) = 0.$$

Suppose that $C$ is of genus one. Then $C$ is birationally equivalent (over a number field) to some elliptic curve

$$E: \quad x^3 + Ax + B = y^2$$

with $A, B \in \mathbb{Q}$. Let $r$ be the rank of $E$, and let $P_1, \dots, P_r$ be a Mordell-Weil basis of $E$. Then any rational point $P$ of $E$ can be written as

$$P = P_0 + n_1 P_1 + \cdots + n_r P_r, \tag{1}$$

where $P_0$ is some torsion point of $E$, and $n_i \in \mathbb{Z}$ $(i = 1, \dots, r)$.

Now on the one hand, using estimates of David [5] concerning linear forms in elliptic logarithms, one gets a lower bound of the form

$$|L(P)| \geq \exp(-c_1(\log N + c_2)(\log\log N + c_3)^{r+3}). \tag{2}$$

Here $L(P)$ is a certain (well-defined) linear form in elliptic logarithms ("roughly" the elliptic logarithm of $P$), $N = \max_{1\le i\le r} |n_i|$ and $c_1, c_2, c_3$ are constants depending only on the curves $C$ and $E$. On the other hand, supposing that $P$ is the image of an integral point of $C$ under the above birational transformation, using standard arguments (including Puiseux expansions, elliptic integrals and height estimates of points of $E$) we get an inequality of the form

$$|L(P)| \le c_4 \exp(-c_5 \lambda N^2). \tag{3}$$

Here $c_4, c_5$ are again constants, which depend only on $C$ and $E$. Furthermore, most importantly from our point of view, $\lambda$ is the least eigenvalue of the height pairing matrix of the basis $P_1, \dots, P_r$ occurring in (1). That is, $\lambda$ certainly depends on the choice of the Mordell-Weil basis. As it is demonstrated by Stroeker and Tzanakis [18], the size of $\lambda$ has a great impact on the final bound $N_{final}$ for $N$. As it turns out, $N_{final}$ is almost linear in $\lambda^{-1/2}$ so it is worth paying attention to this point. We shall return here a little later.

Combining estimates (2) and (3) we get an initial upper bound $N_0$ for $N$. However, this upper bound is usually extremely huge. Due to an observation of Stroeker and Tzanakis [18], $N_0$ should be around $10^{(5r^2+5r+28)/2}$. Hence to explicitly determine the integral points on $C$, this initial bound $N_0$ should be reduced. This can be done by lattice reduction techniques due to de Weger [23], based on the LLL-algorithm. We use a variant due to Tzanakis [21]. To apply this result, one starts with (3), together with the inequality $N < N_0$. Using the appropriate proposition from Section 5 of Tzanakis [21], one gets a new lower bound of the shape

$$N < \frac{c_6}{\sqrt{c_5 \lambda}}$$

for $N$, where $c_6$ is an explicitly computable constant depending on some parameters of $E$, and also on the length of the shortest vector of an LLL-reduced basis of a certain lattice. As one can see, this new bound is linear in $\lambda^{-1/2}$, which shows the importance of this parameter. Stroeker and Tzanakis [18] have considered several examples which indicate this phenomenon in a rather convincing way. Summarizing the results in [18], to get the best possible reduced bound $N_{final}$ for $N$ one should definitely choose an ST-basis of the curve $E$ in (1). Subsequently, Stroeker and Tzanakis [18] have also worked out an efficient algorithm for finding an ST-basis of the curve.

However, in the sequel it turns out that the bound obtained by using an ST-basis, can still be improved further, if one works with several Mordell-Weil bases simultaneously. It is important to note that following our method the use of more bases shall increase only by a fraction of the total time needed to get a better $N_{final}$. As we mentioned in the introduction, a small gain in $N_{final}$ may lead to a large improvement in the searching time for finding the small solutions, in particular, if $r$ is large. The reason is simply that the region where we look for the small solutions is of size $(2N_{final} + 1)^r$. Note that a similar "size" notion was used also in [18] to compare the final bounds obtained in different Mordell-Weil bases.

Now we briefly outline how to work in several bases simultaneously. To explain our ideas it is sufficient to use two bases. So assume that $B_1 = (P_1, \dots, P_r)$ is a Mordell-Weil basis of $E$, and let $S$ be an integral unimodular matrix of size $r \times r$. Let $B_2 = (Q_1, \dots, Q_r)$ be the basis of $E$ obtained from $B_1$ by using $S$ as a basis transformation matrix. Let $P$ be a rational point on $E$ with the representation (1),

and assume that we also have

$$P = Q_0 + m_1 Q_1 + \cdots + m_r Q_r, \tag{4}$$

with some torsion point $Q_0$ and integers $m_1, \ldots, m_r$. Then $Q_0 = P_0$. Put $M = \max_{1 \le i \le r} |m_i|$, and recall that by elementary linear algebra we have

$$S^{-1} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}. \tag{5}$$

This implies $M \le sN$, where $s = ||S^{-1}||$ is the row norm of $S^{-1}$. (The row norm of a $k \times \ell$ type real matrix $A = (a_{ij})_{1 \le j \le \ell, 1 \le i \le k}$ is defined by $||A|| = \max_{1 \le i \le k} \sum_{j=1}^{\ell} |a_{ij}|$.) In particular, this means that one does not have to go through the $\mathcal{E}llog$ method for both $B_1$ and $B_2$, it is sufficient to use it with $B_1$ say. Indeed, take for example $B_1$ to be an ST-basis of $E$, and suppose that after applying the $\mathcal{E}llog$ method (together with the reduction stage) we have the bound $N < N_{final}$. Then by $M \le sN$, we automatically have $M \le M_0 := sN_{final}$. As $s$ is typically "small" (it will be at most around ten), $M_0$ is not too large, and, of course, it can also be reduced. Importantly, we can get the final bound $M_{final}$ very easily and quickly. The reason is that the reduction steps are difficult and time consuming only if the initial bound is large, as then, e.g., high precision is needed. However, as $s$ will be small, the reduction steps leading from $M_0$ to $M_{final}$ are made very easily. The final bounds $N_{final}$ and $M_{final}$ yield simultaneous upper bounds for the coefficients of $P$, in two different bases. Combining these two bounds by (5), we can decrease the domain where the final search has to be done. As one may predict (which turns out to be true), the gain starts getting more and more significant as the rank $r$ becomes larger and larger.

In our calculations we choose $B_1$ to be an ST-basis of $E$, and we choose the other bases according to two different strategies.

*Strategy* 1. We try to decrease $N_{final}^{(1)}$ (corresponding to $B_1$), componentwise. For this purpose, choose distinct indices $i, j$ with $1 \le i, j \le r$ and a positive integer $t$, and consider the bases $B_2$ and $B_3$ obtained by replacing $P_i$ by $P_i + tP_j$ and $P_i - tP_j$ in $B_1$, respectively (leaving the other basis elements untouched). With the bases $B_2$ and $B_3$ the reduction process starts from the quite small bound $(t+1)N_{final}^{(1)}$ and gives, respectively, the final bounds, say, $N_{final}^{(2)}$ and $N_{final}^{(3)}$. Then a simple calculation yields that

$$|n_i| \le \frac{N_{final}^{(2)} + N_{final}^{(3)}}{2t}$$

holds. If the right-hand side happens to be less than $N_{final}^{(1)}$, then we get a new, improved bound for $|n_i|$. To make this principle work, for each fixed $i$ we (heuristically) choose $j$, for which the sum of the $\lambda$ values (corresponding to $B_2$ and $B_3$) is maximal with $t = 1$. Then for simplicity (and also because we try to keep the time consumption of the method low), instead of checking several values, we take the fixed value $t = 10$ in the computations. The procedure can be iterated, and the iteration leads to further improvement in some cases.

Note that the "one-sided" version of this approach could also be used (i.e. when we work only with one of $B_2$ or $B_3$), but our experiences suggest that this "two-sided" version is more efficient. Furthermore, we have some reasons for the choice of $t = 10$. If $\lambda_t$ denotes the value of $\lambda$ corresponding to $t$ (either in $B_2$ or in $B_3$), then $\frac{t+1}{t}\sqrt{\frac{\lambda_t}{\lambda_{t+1}}}$ is close to 1, if $t$ is "large". The value $t = 10$ seems to be large enough to make the $\lambda$s corresponding to $B_2$ and $B_3$ more or less close to each other, and it seems to have some good effect on the outcome. Still, obviously at this point the method can have many variants.

*Strategy* 2. Using the algorithm of Stroeker and Tzanakis [18], we determine the "best" ten Mordell-Weil bases $B_j$ $(j = 1, \dots, 10)$, i.e., ten Mordell-Weil basis corresponding to the ten largest $\lambda$ values. (Note that by the algorithm we get all the basis transformation matrices with respect to $B_1$, as well, and also that the calculation of ten basis takes only a little extra time than calculating only $B_1$.) Then we compute the initial upper bounds $N_0^{(j)}$ $(j = 1, \dots, 10)$ for the coordinates of the integral points in these bases, respectively. (As we mentioned, out of these, only the calculation of $N_0^{(1)}$ is time consuming (but it has to be calculated even if we use only $B_1$), the other bounds come very quickly and easily.) Having these bounds, using the basis transformation matrices, we get several extra information for the coefficients of $P$ in $B_1$. In fact, we get a system of inequalities defining a convex body, which contains many less integral points than the one implied by $|n_i| \le N_{final}^{(1)}$ $(i = 1, \dots, r)$.

Finally, we mention that altogether it seems that *Strategy* 2 yields more improvement than *Strategy* 1.

## 3. Examples

In this section we give some examples, to illustrate how *Strategy* 1 and *Strategy* 2 work. For this purpose we borrow some curves from the papers [18] and [10]. As we mentioned, the problem discussed in the paper is interesting when the rank of the underlying elliptic curve is not too small, so we consider curves of ranks 5 and 6. In fact we have worked out a number of other examples (from [20], [18] and [10]), which can be found on the homepage http://www.math.klte.hu/algebra/hajdu.htm.

In each example we illustrate both *Strategy* 1 and *Strategy* 2. We always start by giving the underlying curve and the basic information corresponding to it. In *Strategy* 1, we give the index $j$ for each $i$, the two corresponding linear inequalities (with $t = 10$, using the notation (1)), and also indicate the final bound obtained for $|n_i|$. Finally, we calculate the improvement ratio, as well.

In *Strategy* 2, we provide the following data. We give the best ten Mordell-Weil bases (in the sense explained above), by using the algorithm of Stroeker and Tzanakis [18]. (Note that the best basis is of course an ST-basis.) The bases are represented by the basis transformation matrices (with respect to the ST-basis). We indicate the corresponding $\lambda$ values, as well. Finally, we list the final bounds in the corresponding bases, obtained by the above mentioned reduction results from [21]. After that we summarize the information in a system of linear inequalities (of the form $-\underline{b} \le A\underline{x} \le \underline{b}$). Using Barvinok's algorithm [2] the number $N^*$ of the integral points in the corresponding convex body can be computed by the program package Latte [11]. Hence we can calculate the "improvement ratio" defined in the

natural way, by $N^*/(2N_{final}+1)^r$, where $N_{final}$ corresponds to the ST-basis. Note that here we may use the reduced bounds obtained for $|n_i|$ by *Strategy* 1.

We give a detailed description only in the first example. In the other examples, we present the data in a brief form, following the previous notation. We start with two curves of rank 5, and we conclude with a rank 6 curve.

**Example 1.** This example is from [18]. We would like to determine the integral points on the curve

$$E: \quad x^3 - 203472x + 18487440 = y^2.$$

The rank of $E$ is $r = 5$, and an ST-basis of $E$ (obtained by the method in [18]) is given by

$$P_1 = (468, 5076), P_2 = (-216, 7236), P_3 = (432, 3348),$$
$$P_4 = (-36, 5076), P_5 = (36, 3348).$$

The final bound obtained for the coordinates of the integral points of $E$ is $N_{final} = 9$ in this basis (see [18]).

*Strategy* 1. Using the above explained methods, we get the following table:

| $i$ | $j$ | bound for $\lvert 10n_i \pm n_j\rvert$ | bound for $\lvert n_i\rvert$ |
|---|---|---|---|
| 1 | 4 | (77,82) | 7 |
| 2 | 1 | (85,79) | 8 |
| 3 | 5 | (76,81) | 7 |
| 4 | 5 | (84,88) | 8 |
| 5 | 1 | (75,81) | 7 |

Based upon the table, the improvement is given by

$$\frac{(2\cdot 7+1)(2\cdot 8+1)(2\cdot 7+1)(2\cdot 8+1)(2\cdot 7+1)}{(2\cdot 9+1)^5} = 0.393916.$$

*Strategy* 2. The basis transformation matrices (with respect to the ST-basis) of the best ten bases (obtained by the method of Stroeker and Tzanakis [18]) are given by

$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ -1&-1&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&1\\ 0&0&0&0&-1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 1&1&-1&1&0\\ 0&0&0&0&1 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 1&1&-1&1&0\\ 1&1&-1&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&0&-1\\ -1&-1&1&1&2\\ 0&-1&1&1&1\\ -1&0&1&1&1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0&1\\ 1&0&0&0&-1\\ 0&1&0&0&0\\ 1&-1&1&0&0\\ 1&-1&1&1&0 \end{pmatrix},$$
$$\begin{pmatrix} 0&0&0&0&1\\ 1&0&0&0&-1\\ 1&1&1&1&0\\ 0&0&-1&-1&0\\ 0&0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0&1\\ 0&0&0&0&-1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 1&1&1&1&0\\ 0&0&0&-1&0\\ 0&0&0&0&1 \end{pmatrix}.$$

The corresponding $\lambda$ values are

$$0.46493, 0.45844, 0.45792, 0.44837, 0.44736,$$
$$0.42425, 0.41358, 0.41295, 0.41229, 0.41173,$$

and the final bounds $N_{final}$ obtained after the reduction are

$$9, 9, 9, 9, 9, 10, 10, 10, 10, 10,$$

respectively. Combining these data, using the notation (1) (with respect to the ST-basis) we get the system of linear inequalities

$$(6)\qquad \begin{pmatrix} -7\\ -8\\ -7\\ -8\\ -7\\ -9\\ -9\\ -9\\ -10\\ -10\\ -10\\ -10 \end{pmatrix} \le \begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 1 & 1 & -1 & -1 & 1\\ -1 & -1 & 1 & 1 & 0\\ 0 & 0 & 0 & -1 & 1\\ -1 & -1 & 1 & 0 & 0\\ -1 & -1 & 0 & 1 & 0\\ 0 & -1 & 1 & 1 & -1\\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} n_1\\ n_2\\ n_3\\ n_4\\ n_5 \end{pmatrix} \le \begin{pmatrix} 7\\ 8\\ 7\\ 8\\ 7\\ 9\\ 9\\ 9\\ 10\\ 10\\ 10\\ 10 \end{pmatrix}.$$

Note that because of some (natural) redundancy, here and also in the other examples, not all the ten basis transformation matrices are needed to derive (6). We also mention that here we can now use the improved upper bounds obtained by *Strategy* 1 for the $|n_i|$. Using Latte [11], we get that the above inequality (6) has precisely $N^* = 396785$ integral solutions in $(n_1, n_2, n_3, n_4, n_5)$. Hence the "improvement ratio" is

$$N^*/(2N_{final}+1)^5 = 396785/(2\cdot 9+1)^5 = 0.160246,$$

where $N_{final} = 9$ corresponds to the ST-basis $P_1, P_2, P_3, P_4, P_5$.

**Example 2.** This example is from [18]. The problem is to find the integral points on the curve

$$E: \quad x^3 - 879984x + 319138704 = y^2.$$

The rank of $E$ is $r = 5$, and an ST-basis of $E$ is given by

$$P_1 = (468, 3132), P_2 = (-684, -24516), P_3 = (720, -7668),$$
$$P_4 = (432, -4428), P_5 = (540, -1188).$$

The final bound obtained for the coordinates of the integral points of $E$ is $N_{final} = 9$ in this basis (cf. [18]).

*Strategy* 1. We obtain the table

| $i$ | $j$ | bound for $\lvert 10n_i \pm n_j\rvert$ | bound for $\lvert n_i\rvert$ |
|---|---|---|---|
| 1 | 5 | (83,79) | 8 |
| 2 | 1 | (76,82) | 7 |
| 3 | 5 | (77,78) | 7 |
| 4 | 3 | (94,89) | 9 |
| 5 | 1 | (79,77) | 7 |

Hence the improvement is given by

$$\frac{(2\cdot 8+1)(2\cdot 7+1)(2\cdot 7+1)(2\cdot 9+1)(2\cdot 7+1)}{(2\cdot 9+1)^5} = 0.440259.$$

*Strategy* 2. The basis transformation matrices of the best ten bases:

$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&1\\ 0&0&1&0&0\\ 0&0&0&0&-1\\ 0&0&0&-1&0\\ 0&-1&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ -1&0&-1&-1&1\\ 0&0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ -1&1&1&0&1\\ 0&-1&0&1&-1\\ 0&0&1&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ -1&0&1&1&-1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&-1&0&1\\ 0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ -1&1&0&1&1\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&0&1&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&0&-1&1\\ 1&1&1&-1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ 1&-1&0&1&1\\ 0&0&0&0&-1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&-1&0&1&-1\\ 0&0&1&0&0 \end{pmatrix}.$$

The corresponding $\lambda$ values are

$$0.492063, 0.462853, 0.457636, 0.454803, 0.454749,$$
$$0.453727, 0.451024, 0.450503, 0.448775, 0.431040,$$

and the final bounds $N_{final}$ obtained after reduction are

$$9, 9, 9, 9, 9, 9, 9, 9, 9, 9,$$

respectively. Thus we get the system of linear inequalities

$$\begin{pmatrix} -8\\ -7\\ -7\\ -9\\ -7\\ -9\\ -9\\ -9 \end{pmatrix} \le \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&-1&1&1&0\\ 1&-1&0&1&0\\ 0&1&-1&-1&1 \end{pmatrix} \begin{pmatrix} n_1\\ n_2\\ n_3\\ n_4\\ n_5 \end{pmatrix} \le \begin{pmatrix} 8\\ 7\\ 7\\ 9\\ 7\\ 9\\ 9\\ 9 \end{pmatrix}.$$

By Latte [11] we obtain that the above inequality has precisely $N^* = 513939$ integral solutions in $(n_1, n_2, n_3, n_4, n_5)$. Hence the "improvement ratio" is

$$513939/(2 \cdot 9 + 1)^5 = 0.207560.$$

**Example 3.** This example is from [10]. The original problem is to find the integral points on the curve

$$C: \quad 2u^3 + 3u^2 + u = 6v^3 + 60v^2 + 144v.$$

The curve is birationally equivalent to

$$E: \quad x^3 - 1008x + 2985993 = y^2.$$

The rank of $E$ is $r = 6$, and an ST-basis of $E$ is

$$P_1 = (-36, 1725), P_2 = (298, 5399), P_3 = (243, 4134),$$
$$P_4 = (-138, -705), P_5 = (24, 1725), P_6 = (-41, 1720).$$

The final bound obtained for the coordinates of the images of the integral points of $C$ on $E$ is $N_{final} = 7$ in this basis (see [10]).

*Strategy* 1. We get the table

| $i$ | $j$ | bound for $\lvert 10n_i \pm n_j \rvert$ | bound for $\lvert n_i \rvert$ |
|---|---|---|---|
| 1 | 3 | (70,68) | 6 |
| 2 | 6 | (69,64) | 6 |
| 3 | 4 | (64,61) | 6 |
| 4 | 3 | (64,60) | 6 |
| 5 | 6 | (68,71) | 6 |
| 6 | 5 | (59,63) | 6 |

Hence the improvement is given by

$$\frac{(2\cdot 6+1)(2\cdot 6+1)(2\cdot 6+1)(2\cdot 6+1)(2\cdot 6+1)(2\cdot 6+1)}{(2\cdot 7+1)^6} = 0.423753.$$

*Strategy* 2. The basis transformation matrices of the best ten bases:

$$\begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} -1&-2&1&-1&1&1\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&-1\\ 0&-1&0&0&1&0\\ 0&-1&0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&-1\\ -1&0&0&0&1&0\\ -1&0&0&0&0&0 \end{pmatrix}, \begin{pmatrix} -1&-1&1&1&0&0\\ 0&0&0&-1&1&0\\ 0&0&0&0&0&1\\ 1&0&-1&-1&1&-1\\ 1&0&0&0&0&0\\ 0&0&0&1&0&0 \end{pmatrix},$$

$$\begin{pmatrix} 0&-1&1&1&1&0\\ -1&0&0&-1&-1&1\\ 0&0&0&0&-1&0\\ 0&0&0&-1&0&0\\ 1&0&0&0&0&0\\ 1&0&1&1&1&-1 \end{pmatrix}, \begin{pmatrix} -1&0&1&-1&1&1\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&-1\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0 \end{pmatrix}, \begin{pmatrix} -1&1&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&1&0&-1&1&1\\ 0&0&1&0&0&0 \end{pmatrix},$$

$$\begin{pmatrix} -1&-1&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&-1&1&-1&1&1\\ 0&1&0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 1&1&-1&1&1&1\\ 0&0&0&0&0&-1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&1&0&0&0\\ 0&1&0&0&0&0\\ -2&-1&1&-1&-1&-1\\ -1&0&0&0&-1&0\\ -1&0&0&0&0&0 \end{pmatrix}.$$

The corresponding $\lambda$ values are

$$0.640325, 0.627020, 0.603695, 0.603010, 0.599688,$$
$$0.595452, 0.587593, 0.586898, 0.586647, 0.586371,$$

and the final bounds $N_{final}$ obtained after reduction are

$$8, 8, 8, 8, 8, 8, 8, 8, 8, 8,$$

respectively. So we get the following system of linear inequalities

$$\begin{pmatrix} -6\\-6\\-6\\-6\\-6\\-6\\-8\\-8\\-8\\-8\\-8\\-8\\-8 \end{pmatrix} \le \begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ -1&1&-1&-1&1&1\\ 0&0&0&0&1&-1\\ -1&1&-1&-1&0&1\\ 0&1&-1&-1&1&0\\ 0&1&0&0&0&1\\ -1&1&-1&-1&1&0\\ 0&1&-1&-1&1&1 \end{pmatrix} \begin{pmatrix} n_1\\n_2\\n_3\\n_4\\n_5\\n_6 \end{pmatrix} \le \begin{pmatrix} 6\\6\\6\\6\\6\\6\\8\\8\\8\\8\\8\\8\\8 \end{pmatrix}.$$

Latte [11] gives that the above system has precisely $N^* = 1801039$ integral solutions in $(n_1, n_2, n_3, n_4, n_5, n_6)$. Thus the "improvement ratio" is

$$1801039/(2\cdot 7+1)^6 = 0.158116.$$

## Acknowledgement

The authors are grateful to the referee for the useful and helpful remarks.

## References

1. A. Baker, *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. **43** (1968), 1–9. MR0231783 (38:111)
2. A. I. Barvinok, *A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed*, in 34th Annual Symposium of Foundations of Computer Science, pp. 566–572, IEEE, Nov. 1993. MR1328451
3. Y. Bugeaud, *On the size of integer solutions of elliptic equations*, Bull. Austral. Math. Soc. **57** (1998), 199–206. MR1617363 (99h:11027)
4. Y. Bugeaud, *On the size of integer solutions of elliptic equations* II, Bull. Greek Math. Soc. **43** (2000), 125–130. MR1846953 (2002e:11030)

5. S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Soc. Math. France, Mémoire 62 (Suppl. Bull. S. M. F.) **123** (1995), pp. 143. MR1385175 (98f:11078)
6. J. Gebel, A. Pethő, H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192. MR1305199 (95i:11020)
7. L. Hajdu, *Optimal systems of fundamental S-units for LLL-reduction* (to appear).
8. L. Hajdu, T. Herendi, *Explicit bounds for the solutions of elliptic equations with rational coefficients*, J. Symbolic Computation **25** (1998), 361–366. MR1615334 (99a:11033)
9. L. Hajdu, T. Kovács, *A parallel LLL-reduction method for bounding the solutions of S-unit equations* (manuscript).
10. T. Kovács, *Combinatorial Diophantine equations—the genus 1 case*, Publ. Math. Debrecen **72** (2008), no. 1–2, 243–255. MR2376872
11. J. A. De Loera, D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, R. Yoshida, *A user's guide for LattE v1.1*, Nov. 2003.
12. Á. Pintér, *On the magnitude of integer points on elliptic curves*, Bull. Austral. Math. Soc. **52** (1995), 195–199. MR1348477 (96k:11070)
13. D. Poulakis, *Integral points on algebraic curves with exceptional units*, J. Austral. Math. Soc. Ser. A **63** (1997), 145–164. MR1475559 (98k:11088)
14. W. M. Schmidt, *Integer points on curves of genus 1*, Compositio Math. **81** (1992), 33–59. MR1145607 (93e:11076)
15. T. N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986. MR891406 (88h:11002)
16. V. G. Sprindžuk, *Classical Diophantine Equations*, Lecture Notes in Math. **1559**, Springer-Verlag, Berlin, 1993. MR1288309 (95g:11017)
17. R. J. Stroeker, N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), 177–196. MR1291875 (95m:11056)
18. R. J. Stroeker, N. Tzanakis, *On the elliptic logarithm method for elliptic Diophantine equations: Reflections and an improvement*, Experimental Math. **8** (1999), 135–149. MR1700575 (2000d:11043)
19. R. J. Stroeker, N. Tzanakis, *Computing all integer solutions of a genus 1 equation*, Math. Comp. **72** (2003), 1935–1946. MR1986812 (2004b:11037)
20. R. J. Stroeker, B. M. M. de Weger, *Elliptic binomial Diophantine equations*, Math. Comp. **68** (1999), 1257–1281. MR1622097 (99i:11122)
21. N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, Acta Arith. **75** (1996), 165–190. MR1379397 (96m:11019)
22. P. M. Voutier, *An upper bound for the size of integer solutions to* $Y^m = f(X)$, J. Number Theory **53** (1995), 247–271. MR1348763 (96f:11049)
23. B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam, 1989. MR1026936 (90m:11205)

University of Debrecen, Institute of Mathematics, and the Number Theory Research Group of the Hungarian Academy of Sciences, P.O. Box 12, H-4010 Debrecen, Hungary
*E-mail address*: hajdul@math.klte.hu

University of Debrecen, Institute of Mathematics, P.O. Box 12, H-4010 Debrecen, Hungary
*E-mail address*: tundekov@gmail.com