ACTA ARITHMETICA
LXVIII.2 (1994)

# Computing integral points on elliptic curves

by

J. Gebel (Saarbrücken), A. Pethő (Debrecen)
and H. G. Zimmer (Saarbrücken)

**1. Introduction.** By a famous theorem of Siegel [S], the number of integral points on an elliptic curve $E$ over an algebraic number field $\mathbb{K}$ is finite. A conjecture of Lang and Demyanenko (see [L3], p. 140) states that, for a quasiminimal model of $E$ over $\mathbb{K}$, this number is bounded by a constant depending only on the rank of $E$ over $\mathbb{K}$ and on $\mathbb{K}$ (see also [HSi], [Zi4]). This conjecture was proved by Silverman [Si1] for elliptic curves with integral modular invariant $j$ over $\mathbb{K}$ and by Hindry and Silverman [HSi] for algebraic function fields $\mathbb{K}$. On the other hand, beginning with Baker [B], effective bounds for the size of the coefficients of integral points on $E$ have been found by various authors (see [L4]). The most recent bound was established by W. Schmidt [Sch, Th. 2]. However, the bounds are rather large and therefore can be used only for solving some particular equations (see [TdW1], [St]) or for treating a special model of elliptic curves, namely Thue curves of degree 3 (see [GSch]). The Siegel–Baker method (see [L3]) for the calculation of integer points on elliptic curves over $\mathbb{K} = \mathbb{Q}$ requires some detailed information about certain quartic number fields. Computing these fields often represents a hard problem and, moreover, this approach does not seem to be appropriate. That is why in general all the results mentioned above cannot be used for the actual calculation of *all* integral points on an elliptic curve $E$ over $\mathbb{Q}$.

However, there is another method suggested by Lang [L1], [L3] and further developed by Zagier [Za]. We shall work out the Lang–Zagier method and turn it into an algorithm for determining all integral points on elliptic curves $E$ over $\mathbb{Q}$ using elliptic logarithms. The algorithm requires the knowledge of a basis of the Mordell–Weil group $E(\mathbb{Q})$ and of an explicit lower bound for linear forms in elliptic logarithms. Compared to the Siegel–Baker

This work was partially supported by the Deutsche Forschungsgemeinschaft, the Hungarian Academy of Sciences and the Siemens AG.

method, it thus appears to be more natural and suitable for the problem under consideration. The examples given at the end of the paper show that our algorithm is also very efficient: we were able to compute all integer points on certain elliptic curves over $\mathbb{Q}$ of ranks up to at least six.

As mentioned above, our method requires the knowledge of a basis of the Mordell–Weil group $E(\mathbb{Q})$. Actually, this is the only disadvantage of the Lang–Zagier method. However, an algorithm providing such a basis was recently developed by the first and the last author [GZ]. It is based on ideas of Manin [M] and depends on the validity of the conjecture of Birch and Swinnerton-Dyer (see [F], [Zi3], for example). We are planning to make it independent of this conjecture. The second component is an explicit lower bound for linear forms in elliptic logarithms of algebraic numbers. Again it was only recently that S. David [D] established such an explicit bound, thus proving another conjecture of Lang. This meant a breakthrough in our endeavor concerning integral points. Analogous estimates for linear forms in complex and $p$-adic logarithms had been successfully used for the complete resolution of Thue, Thue–Mahler and index form equations (see [PS], [TdW1], [TdW2], [GPP]). The reduction procedure, based on numerical diophantine approximation techniques, is the third important component of our method. We shall use here a variant given by de Weger [dW].

**2. Heights.** The elliptic curve $E$ over $\mathbb{Q}$ is assumed to be given in *short Weierstrass normal form*

$$E: \quad y^2 = x^3 + ax + b =: p(x) \qquad (a, b \in \mathbb{Z}). \tag{1}$$

The *discriminant* of $E$ over $\mathbb{Q}$ is

$$\Delta = 4a^3 + 27b^2 \neq 0$$

and the *modular invariant*

$$j = 12^3 \frac{4a^3}{\Delta}.$$

By the Mordell–Weil Theorem, the group $E(\mathbb{Q})$ is finitely generated, hence is the product

$$E(\mathbb{Q}) \cong E_{\mathrm{tors}}(\mathbb{Q}) \times \mathbb{Z}^r$$

of the finite *torsion group* $E_{\mathrm{tors}}(\mathbb{Q})$ and an infinite part isomorphic to $r$ copies of the rational integers $\mathbb{Z}$, where $r$ denotes the *rank* of $E$ over $\mathbb{Q}$.

Let us recall the notion of height on $E(\mathbb{Q})$. For a rational point

$$P = (\xi/\zeta^2, \eta/\zeta^3) \in E(\mathbb{Q}),$$

where $\xi, \eta, \zeta \in \mathbb{Z}$ and $\gcd(\xi, \zeta) = \gcd(\eta, \zeta) = 1$, the *ordinary height* or *Weil height* is

$$h(P) = \begin{cases} \frac{1}{2} \log \max\{\zeta^2, |\xi|\} & \text{if } P \neq \mathcal{O}, \\ 0 & \text{if } P = \mathcal{O}, \end{cases}$$

where $\mathcal{O}$ is the point at infinity. The *canonical height* or *Néron–Tate height* of $P$ is then the limit

$$\widehat{h}(P) := \lim_{n\to\infty} h(2^n P)/2^{2n}.$$

Note that $\widehat{h}$ is a positive semidefinite quadratic form on $E(\mathbb{Q})$ and that the null space of $\widehat{h}$ is simply the torsion group $E_{\mathrm{tors}}(\mathbb{Q})$. Therefore, $\widehat{h}$ is a positive definite quadratic form on the factor group

$$\overline{E}(\mathbb{Q}) := E(\mathbb{Q})/E_{\mathrm{tors}}(\mathbb{Q}).$$

By embedding $\overline{E}(\mathbb{Q})$ in the $r$-dimensional real space $\mathcal{E}(\mathbb{R}) := E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$, it is clear that $\widehat{h}$ extends to a positive definite quadratic form $\widehat{h}$ on $\mathcal{E}(\mathbb{R}) \cong \mathbb{R}^r$ and thus gives rise to a *Euclidean norm* on $\mathcal{E}(\mathbb{R})$. In the Euclidean space $\mathcal{E}(\mathbb{R})$ with respect to this norm, a basis of the Mordell–Weil group $E(\mathbb{Q})$ can be found by methods taken from geometry of numbers (see [M], [GZ]).

Let $P_1, \ldots, P_r \in E(\mathbb{Q})$ denote such a basis (of the infinite part) of $E(\mathbb{Q})$. Then each rational point $P \in E(\mathbb{Q})$ has a unique representation of the form

$$P = \sum_{i=1}^{r} n_i P_i + P_{r+1} \quad (n_i \in \mathbb{Z}), \tag{2}$$

where $P_{r+1} \in E_{\mathrm{tors}}(\mathbb{Q})$ is a torsion point.

We want to get rid of $P_{r+1}$ in (2). To this end, we multiply both sides of (2) by the order $g \in \mathbb{N}$ of $P_{r+1}$. This yields for the multiple $P' = gP$ of $P$ the representation

$$P' = \sum_{i=1}^{r} n_i' P_i \quad (n_i' = g n_i \in \mathbb{Z}). \tag{2'}$$

Note that, by a famous theorem of Mazur [Mz], we have

$$g \le 12. \tag{3}$$

Of course, in practice we can precompute $g$ and use it instead of the upper bound 12. In particular, if $E$ over $\mathbb{Q}$ has no torsion, we take $g = 1$.

In order to compute all integral points

$$P = (\xi, \eta) \in E(\mathbb{Q}), \quad \text{where } \zeta = 1,$$

we must find an upper bound for the coefficients $n_i$ in the representation (2) of $P$ by the basis points $P_i$ $(i = 1, \ldots, r)$. Put

$$N := \max_{1\le i\le r} \{|n_i|\}. \tag{4}$$

Let us look at the representation (2) modulo torsion, viz.

$$\overline{P} = \sum_{i=1}^{r} n_i \overline{P}_i,$$

and consider the embedding $\overline{E}(\mathbb{Q}) \hookrightarrow \mathcal{E}(\mathbb{R}) \cong \mathbb{R}^r$. Since $\widehat{h}$ is a positive definite quadratic form on the Euclidean space $\mathcal{E}(\mathbb{R})$, we obtain the lower estimate (cf. [G], Th. 10, p. 319)

$$\widehat{h}(P) \geq \lambda_1 N^2 \tag{5}$$

on non-torsion points $P \in E(\mathbb{Q})$, where $0 < \lambda_1 \in \mathbb{R}$ is the smallest eigenvalue of the matrix associated with $\widehat{h}$ and the given basis $P_1, \ldots, P_r$ of $E(\mathbb{Q})$.

Next we are going to replace in (5) the canonical height $\widehat{h}$ by a modified ordinary height $d$ to be used in place of $h$. This is accomplished by means of an estimate between $\widehat{h}$ and $d$ on $E(\mathbb{Q})$. The *modified ordinary height* of a point $P = (\xi/\zeta^2, \eta/\zeta^3) \in E(\mathbb{Q})$ is defined as (cf. [Zi1]–[Zi3], [Zi5])

$$d(P) := \begin{cases} \frac{1}{2}\max\{\mu_\infty + 2\log\zeta,\ \log|\xi|\} & \text{if } P \neq \mathcal{O}, \\ \frac{1}{2}\mu_\infty & \text{if } P = \mathcal{O}, \end{cases}$$

with the "height" of $E$

$$\mu_\infty := \log\max\{|a|^{1/2}, |b|^{1/3}\} \tag{6}$$

given in terms of the coefficients $a, b \in \mathbb{Z}$ of the elliptic curve $E$. The following estimate for the difference $d - \widehat{h}$ on $E(\mathbb{Q})$ was established in [Zi2], [Zi3] (cf. also [Zi1], [Si2]):

$$-\tfrac{2}{3}\log 2 \leq d(P) - \widehat{h}(P) \leq \tfrac{3}{2}\mu_\infty + \tfrac{5}{3}\log 2. \tag{7}$$

In fact, on combining the height estimates obtained in [Zi2] and [Zi3] with those from [Zi5], one ends up with the slightly stronger estimate

$$-\tfrac{7}{12}\log 2 \leq d(P) - \widehat{h}(P) \leq \tfrac{3}{2}\mu_\infty + \tfrac{19}{12}\log 2. \tag{7$'$}$$

For the sake of simplicity, however, we shall use (7) rather than (7′). (Note that the height $d$ in [Zi1]–[Zi3] differs from the $d$ defined above by a factor of 3.)

From (7) we derive

$$d(P) \geq \widehat{h}(P) - \tfrac{2}{3}\log 2.$$

Hence, for sufficiently large *integral* points $P = (\xi, \eta) \in E(\mathbb{Q})$, more precisely, for points $P$ such that $\zeta = 1$ and $\log|\xi| > \mu_\infty$, we have

$$\tfrac{1}{2}\log|\xi| \geq \widehat{h}(P) - \tfrac{2}{3}\log 2. \tag{8}$$

Combining (5) and (8) yields

$$\tfrac{1}{2}\log|\xi| \geq \lambda_1 N^2 - \tfrac{2}{3}\log 2. \tag{9}$$

We remark that if $\mu_\infty$ is large, e.g. $\exp(\mu_\infty) > 10^6$, and if $0 \leq \log|\xi| \leq \mu_\infty$, we must refine the estimates (7)–(9) as follows. It is easy to see that, for integral points $P \in E(\mathbb{Q})$, we have $0 \leq d(P) - h(P) \leq \frac{1}{2}\mu_\infty$. Combining

these inequalities with (7) yields

$$(7'') \qquad -\tfrac{2}{3}\log 2 - \tfrac{1}{2}\mu_\infty \le h(P) - \widehat{h}(P) \le \tfrac{3}{2}\mu_\infty + \tfrac{5}{3}\log 2.$$

From (7″) we get the lower estimate $h(P) \ge \widehat{h}(P) - \frac{2}{3}\log 2 - \frac{1}{2}\mu_\infty$ and hence

$$(8') \qquad \tfrac{1}{2}\log|\xi| \ge \widehat{h}(P) - \tfrac{2}{3}\log 2 - \tfrac{1}{2}\mu_\infty.$$

Therefore, in the case of $0 \le \log|\xi| \le \mu_\infty$, (9) is to be replaced by the weaker inequality

$$(9') \qquad \tfrac{1}{2}\log|\xi| \ge \lambda_1 N^2 - \tfrac{2}{3}\log 2 - \tfrac{1}{2}\mu_\infty.$$

This case requires an extra search.

We confine ourselves to explaining the search procedure for *large* integral points $P = (\xi,\ \eta) \in E(\mathbb{Q})$ for which the stronger bound in (9) can be used.

**3. Elliptic logarithms.** The next step consists of inserting in (9) the elliptic logarithm of $P$ by using the Weierstrass parametrization of our elliptic curve $E$ (see [L2], for example). There exists a lattice $\Omega \subseteq \mathbb{C}$ such that the group of complex points is

$$E(\mathbb{C}) \cong \mathbb{C}/\Omega,$$

where $\Omega = \langle \omega_1, \omega_2 \rangle$ is generated by two *fundamental periods* $\omega_1$ and $\omega_2$ of which $\omega_1$ is real and $\omega_2$ complex. We put $\tau = \omega_2/\omega_1$ and assume, without loss of generality, that $\mathrm{Im}(\tau) > 0$. The above isomorphism is defined by Weierstrass' $\wp$-function with respect to $\Omega$ and its derivative $\wp'$ according to the assignment

$$P = (\wp(u), \wp'(u)) \leftarrow\!\shortmid\, u \bmod \Omega,$$

so that the coordinates of an integral point $P = (\xi, \eta) \in E(\mathbb{Q})$ are given by

$$\xi = \wp(u), \qquad \eta = \wp'(u).$$

Let $\alpha \in \mathbb{R}$ be the largest real root of the right hand side of the Weierstrass equation, i.e. of the polynomial $p(x)$ in (1). Then the real period $\omega_1$ of $E$ is (cf. [Za])

$$(10) \qquad \omega_1 = 2\int_\alpha^\infty \frac{dx}{\sqrt{x^3 + ax + b}}.$$

The elliptic logarithm of $P = (\xi, \eta) \in E(\mathbb{Q})$ is (cf. [Za])

$$(11) \qquad u \equiv \frac{1}{\omega_1}\int_\xi^\infty \frac{dx}{\sqrt{x^3 + ax + b}} \pmod{\mathbb{Z}}.$$

Let $\beta$, $\gamma \in \mathbb{C}$ be the other roots of $p(x)$. Put

$$M := \begin{cases} 0 & \text{if } \alpha \geq 0, \\ \dfrac{\exp(\mu_\infty)}{\sqrt[3]{2}-1} & \text{if } \alpha < 0 \end{cases} \tag{12}$$

and choose a real number

$$\xi_0 := \begin{cases} 2\alpha + M & \text{if } \beta, \gamma \in \mathbb{R}, \\ 2\max\{\alpha, (\beta+\gamma)/2\} + M & \text{if } \beta, \gamma \in \mathbb{C}\backslash\mathbb{R}. \end{cases} \tag{13}$$

In order to estimate the elliptic logarithm of the point $P = (\xi, \eta) \in E(\mathbb{Q})$, we need the following auxiliary result.

Lemma 1. *Suppose that the first coordinate of the integral point* $P = (\xi, \eta) \in E(\mathbb{Q})$ *satisfies*

$$\xi > \max\{0, \xi_0\}.$$

*Then*

$$\int_{\xi}^{\infty} \frac{dx}{\sqrt{x^3 + ax + b}} < \frac{\sqrt{8}}{\sqrt{\xi}}. \tag{14}$$

Remark. If $\xi < 0$, then it must be bounded in absolute value since otherwise $p(\xi)$ could not be a square. An extra search will take care of this case, too.

We shall prove this lemma later and proceed instead in solving our task of estimating elliptic logarithms. Normalizing the value of $u$ in (11) to $0 < |u| \leq 1/2$ and assuming $\xi > \max\{0, \xi_0\}$, we obtain from (11) and (14) the estimate

$$|u| < \frac{\sqrt{8}}{\omega_1} \cdot \frac{1}{\sqrt{|\xi|}}. \tag{15}$$

On combining (9) and (15), we get

$$\log|u| < \log\sqrt{8} - \log\omega_1 - \lambda_1 N^2 + \tfrac{2}{3}\log 2.$$

Exponentiating leads to

$$|u| < c_1' \exp\{-\lambda_1 N^2\} \tag{16}$$

for

$$c_1' := \frac{2\sqrt{2} \cdot \sqrt[3]{4}}{\omega_1}. \tag{17}$$

Now we are going to apply the crucial Theorem 2.1 of David ([D]). Written in terms of elliptic logarithms, equation (2) reads

$$u \equiv \sum_{i=1}^{r} n_i u_i + u_{r+1} \pmod{\mathbb{Z}},$$

where $u_{r+1}$ is the elliptic logarithm of the torsion point $P_{r+1} \in E_{\text{tors}}(\mathbb{Q})$ and, for $1 \le i \le r$, the $u_i$'s are the elliptic logarithms of the basis points $P_i \in E(\mathbb{Q})$. Rewritten as an equality, this congruence becomes

$$u = n_0 + \sum_{i=1}^{r} n_i u_i + u_{r+1} \tag{18}$$

for some integer $n_0 \in \mathbb{Z}$. If we replace (2) by (2′), we obtain for the elliptic logarithm $u' = gu$ of the point $P' = gP \in E(\mathbb{Q})$ the representation

$$u' = n_0' + \sum_{i=1}^{r} n_i' u_i \quad (n_i' = g n_i \in \mathbb{Z}) \tag{18′}$$

which we shall use instead of (18). Of course, (16) is then to be replaced by

$$|u'| < g c_1' \exp\{-\lambda_1 N^2\}. \tag{16′}$$

Here again we assume the elliptic logarithms normalized to

$$0 < |u_i| \le \tfrac{1}{2} \quad (1 \le i \le r). \tag{19}$$

Since David works with the classical Weierstrass form

$$E: \quad y^2 = 4x^3 - g_2 x - g_3,$$

we must rearrange it to get

$$E: \quad (\tfrac{1}{2}y)^2 = x^3 - \tfrac{1}{4}g_2 x - \tfrac{1}{4}g_3$$

so that we have $g_2 = -4a,\ g_3 = -4b$. Hence, the height $h$ in [D] becomes

$$\begin{aligned} h &= h(1, g_2, g_3, j) \\ &= h(1, -4a, -4b, j) \\ &= \sum_p \log \max\{1, |4a|_p, |4b|_p, |j|_p\} + \log \max\{1, |4a|, |4b|, |j|\}, \end{aligned}$$

where the summation is over all rational primes $p$ of $\mathbb{Q}$, and $|\ |_p$ denotes the normalized multiplicative $p$-adic valuation and $|\ |$ the ordinary absolute value on $\mathbb{Q}$. Writing the modular invariant in shortest terms $j = j_1/j_2$ for $j_1, j_2 \in \mathbb{Z}$ and using the sum formula

$$\sum_p \log |x|_p + \log |x| = 0 \quad (0 \ne x \in \mathbb{Q}),$$

we obtain for $h$ the expression

$$\begin{aligned} h &= h(1, -4a, -4b, j_1/j_2) \\ &= \sum_p \max\{0, \log |4a|_p, \log |4b|_p, \log |j_1|_p - \log |j_2|_p\} \\ &\quad + \max\{0, \log |4a|, \log |4b|, \log |j_1| - \log |j_2|\} \end{aligned} \tag{20}$$

$$
\begin{aligned}
&= -\sum_p \min\{-\log|j_2|_p, -\log|4aj_2|_p, -\log|4bj_2|_p, -\log|j_1|_p\} \\
&\quad + \max\{\log|j_2|, \log|4aj_2|, \log|4bj_2|, \log|j_1|\} \\
&= \log\max\{4|aj_2|, 4|bj_2|, |j_1|, |j_2|\},
\end{aligned}
$$

since $a$, $b$, $j_1$, $j_2$ are integers and $j_1$, $j_2$ are relatively prime. Therefore, we take the expression (20) as the value $h$ in David's Theorem 2.1. Furthermore, we choose $D := 1$ and real numbers $V_1, \dots, V_r$ and $B$ such that, in accordance with (2) and (2′),

$$
\log V_i \geq \max\left\{\widehat{h}(P_i), h, \frac{3\pi|u_i|^2}{\omega_1^2 \mathrm{Im}(\tau)}\right\} \quad \text{for } 1 \leq i \leq r \tag{21}
$$

and, a fortiori,

$$
B \geq V := \max_{1\leq i\leq r}\{V_i\}. \tag{22}
$$

It turns out to be necessary to impose another condition on $B$. To this end, note that by the definition (4) of $N$, we have for the coefficients $n_i'$ in (2′) the estimates

$$
|n_i'| \leq gN \quad \text{for } 1 \leq i \leq r. \tag{4′}
$$

On the other hand, the integer $n_0'$ in (18′) can be estimated as follows. On inserting in (16′) the expression (18′) for $u'$ we get

$$
\left|n_0' + \sum_{i=1}^r n_i' u_i\right| < gc_1' \exp\{-\lambda_1 N^2\},
$$

and the right hand side can be made $\leq 1/2$ for sufficiently large $N$, namely for

$$
N \geq \sqrt{\frac{\log(2gc_1')}{\lambda_1}}. \tag{23}
$$

Hence, we obtain

$$
\begin{aligned}
|n_0'| &= \left|n_0' + \sum_{i=1}^r n_i' u_i - \sum_{i=1}^r n_i' u_i\right| \leq \left|n_0' + \sum_{i=1}^r n_i' u_i\right| + \left|\sum_{i=1}^r n_i' u_i\right| \\
&\leq \frac{1}{2} + \sum_{i=1}^r |n_i'||u_i| \leq \frac{1}{2} + \frac{r}{2} gN \leq \frac{r+1}{2} gN
\end{aligned}
$$

by the normalization (19) of the $u_i$'s and by (4′), (23). Therefore, assuming (23) and $N > e^e$, we choose

$$
B := \frac{r+1}{2} gN, \tag{24}
$$

keeping in mind that condition (22) must also be satisfied.

Finally, we introduce the constant (see [D])

$$C := 1.1 \cdot 10^9 \cdot 10^{7r}(2/e)^{2r^2}(r+1)^{4r^2+10r}. \tag{25}$$

On combining the estimate (16′) with David's Theorem 2.1 and observing the relations (21)–(25), we arrive at the following important result.

PROPOSITION. *The elliptic logarithm*

$$u = n_0 + \sum_{i=1}^{r} n_i u_i + u_{r+1}$$

*of an integral point* $P = (\xi, \eta) = (\wp(u), \wp'(u)) \in E(\mathbb{Q})$ *such that*

$$\xi > \max\{e^{\mu_\infty}, \xi_0\}$$

*with* $\mu_\infty$ *from* (6) *and* $\xi_0$ *as in* (13) *satisfies the estimate*

$$\exp\left\{-Ch^{r+1}\left(\log\left(\frac{r+1}{2}gN\right)+1\right)\left(\log\log\left(\frac{r+1}{2}gN\right)+1\right)^{r+1}\prod_{i=1}^{r}\log V_i\right\}$$
$$\le |gu| < \exp\{-\lambda_1 N^2 + \log(gc_1')\},$$

*where* $N = \max_{1\le i\le r}\{|n_i|\}$ *as in* (4), *the constants* $\lambda_1$ *and* $c_1'$ *are given as in* (5) *and* (17), *respectively, and* $g \in \mathbb{N}$ *is subject to* (3).

Taking logarithms and omitting the middle term $\log|gu|$, we conclude that the following inequality holds.

COROLLARY. *Under the hypothesis of the proposition*,

$$Ch^{r+1}\left(\log\left(\frac{r+1}{2}gN\right)+1\right)\left(\log\log\left(\frac{r+1}{2}gN\right)+1\right)^{r+1} \times \prod_{i=1}^{r}\log V_i + \log(gc_1') > \lambda_1 N^2. \tag{26}$$

**4. A bound for integral points.** Of course, the inequality (26) can hold only for a finite set of positive integers $N$. We wish to determine a bound for those numbers $N$ and hence for the coefficients $n_i$ in the representation (2) of integral points $P \in E(\mathbb{Q})$. For this purpose, we first state another lemma.

LEMMA 2. *Let* $\varrho$, $\delta$ *and* $\sigma$ *be real numbers satisfying*

$$\varrho \ge 1, \quad \delta \ge 1 \quad \textit{and} \quad \sigma > \max\{(e^2/\delta)^\delta, 1\}.$$

*Then the largest solution* $x_0 \in \mathbb{R}$ *of the equation* $x = \varrho + \sigma \log^\delta x$ *satisfies the inequality*

$$x_0 < 2^{2\delta}\varrho\sigma\log^\delta(\sigma\delta^\delta).$$

Again, we postpone the proof of Lemma 2 and instead apply it to our situation. If

$$N > \max\{e^e, (6r+6)^2\}, \tag{27}$$

we have in (26) the inequality

$$\left(\log\left(\frac{r+1}{2}gN\right)+1\right)\left(\log\log\left(\frac{r+1}{2}gN\right)+1\right)^{r+1} < 2\log^{r+2} N = 2^{-(r+1)}\log^{r+2} N^2. \tag{28}$$

Observing (17) and (25), we put

$$c_1 := \max\left\{\frac{\log(gc_1')}{\lambda_1}, 1\right\}, \quad c_2 := \max\left\{\frac{C}{\lambda_1}, 10^9\right\}\left(\frac{h}{2}\right)^{r+1}\prod_{i=1}^{r}\log V_i. \tag{29}$$

On replacing in (26) the middle term by the right hand side of (28), we derive from (26) the inequality

$$N^2 < c_1 + c_2\log^{r+2} N^2. \tag{30}$$

Now we apply Lemma 2 to (30). Let $N_0 \in \mathbb{R}$ be the largest solution of the equation obtained by equating both sides of (30). Then (30) cannot hold for $N > N_0$. Taking

$$\varrho := c_1, \quad \sigma := c_2 \quad \text{and} \quad \delta := r+2$$

and observing that the hypothesis of Lemma 2 is satisfied, we infer from Lemma 2 for $N_0$ the estimate

$$N_0 < N_1 := 2^{r+2}\sqrt{c_1c_2}\log^{(r+2)/2}(c_2(r+2)^{r+2}). \tag{31}$$

It is clear that the positive integers $N$ satisfying (30) also satisfy (31) since, as we noted, (30) implies $N \le N_0$. Of course, by the conditions (23) and (27) on $N$, we also have

$$N_1 > \max\left\{e^e, (6r+6)^2, \sqrt{\frac{\log(2gc_1')}{\lambda_1}}\right\}. \tag{32}$$

On combining the relations (3), (22), (24) and (31), we thus arrive at the following fundamental theorem.

THEOREM. *Let*

$$P = \sum_{i=1}^{r} n_iP_i + P_{r+1} \in E(\mathbb{Q})$$

*be an integral point on the elliptic curve $E$ over $\mathbb{Q}$, where $P_1, \dots, P_r \in E(\mathbb{Q})$ form a basis of the infinite part of $E(\mathbb{Q})$ and $P_{r+1} \in E_{\mathrm{tors}}(\mathbb{Q})$ is a torsion point. Then the maximum*

$$N = \max_{1\le i\le r}\{|n_i|\}$$

*satisfies the inequality*

$$N \le N_2 := \max\left\{N_1, \frac{2V}{r+1}\right\},$$

*where* $N_1$ *is defined by* (31) *and* $V$ *is given by* (22) *with the* $V_i$*'s subject to* (21).

Based on this theorem, we have developed an algorithm which computes all integral points on any elliptic curve $E$ over $\mathbb{Q}$ of not too high rank. As pointed out already, the algorithm works well for curves $E$ of ranks up to six over $\mathbb{Q}$. However, any improvement of David's bound in [D] would make it possible to treat elliptic curves of still higher ranks.

It remains to prove the two lemmata, to explain how to calculate the elliptic logarithms $u_i$ of the basis points $P_i$ as well as the real and complex period $\omega_1$ and $\omega_2$, respectively, so that the $V_i$'s can be determined in accordance with (21), and to show how the bound in the Theorem can be reduced to facilitate the computation of all integral points in $E(\mathbb{Q})$.

## 5. Proofs

P r o o f  o f  L e m m a 1. We may assume without loss of generality that the largest real root $\alpha \in \mathbb{R}$ of the polynomial $p(x)$ in (1) is non-negative. For if $\alpha$ is negative, we translate $p$ by a suitable positive number $M$ as follows. By the estimate given by Zassenhaus [Zs], we have

$$|\alpha| \le \frac{|p|}{\sqrt[3]{2}-1} \le \frac{e^{\mu_\infty}}{\sqrt[3]{2}-1},$$

since, by (6),

$$|p| := \max\left\{\sqrt{|a|/3}, \sqrt[3]{|b|}\right\} \le \max\left\{\sqrt{|a|}, \sqrt[3]{|b|}\right\} = e^{\mu_\infty}.$$

Then the polynomial $q(y) := p(y-M)$ in $y := x + M$ with $M$ as in (12) has the largest real root $\alpha + M \ge 0$. Choose $\xi_0 \in \mathbb{R}$ in accordance with (13) and suppose that $\xi \in \mathbb{R}$ satisfies

$$\xi > \max\{0, \xi_0\}. \tag{33}$$

Our integral becomes

$$\int_{\xi}^{\infty} \frac{dx}{\sqrt{p(x)}} = \int_{\xi+M}^{\infty} \frac{dy}{\sqrt{q(y)}}.$$

Next we move the root $\alpha + M$ of $q(y)$ to zero by introducing the polynomial in $z := y - (\alpha + M)$,

$$r(z) := q(z + (\alpha + M)) = z(z + \beta_1)(z + \gamma_1)$$

for

$$\beta_1 := \alpha - \beta, \qquad \gamma_1 := \alpha - \gamma.$$

The integral becomes

$$\int_{\xi}^{\infty} \frac{dx}{\sqrt{p(x)}} = \int_{\xi-\alpha}^{\infty} \frac{dz}{\sqrt{r(z)}} = \int_{\xi-\alpha}^{\infty} \frac{dz}{\sqrt{z(z+\beta_1)(z+\gamma_1)}}.$$

We consider two cases:

1. Suppose that either $\beta, \gamma \in \mathbb{R}$ or $\beta, \gamma \in \mathbb{C}\backslash\mathbb{R}$ but $\beta + \gamma = \beta + \overline{\beta} < 2\alpha$. Then $\beta_1 > 0$ and $\gamma_1 > 0$ under the first condition and $\beta_1 + \gamma_1 = \beta_1 + \overline{\beta}_1 = 2\alpha - \beta - \overline{\beta} > 0$ under the second. Under both conditions we find that $r(z) > z^3$ for $z > 0$ ($\Leftrightarrow y > \alpha + M \Leftrightarrow x > \alpha$), and hence conclude that

$$\int_{\xi-\alpha}^{\infty} \frac{dz}{\sqrt{r(z)}} < \int_{\xi-\alpha}^{\infty} \frac{dz}{z^{3/2}} = \frac{2}{\sqrt{\xi-\alpha}}. \tag{34}$$

Now if $\beta, \gamma \in \mathbb{R}$, we derive from $\xi/2 > \alpha + M/2$ by (13) and (33) that

$$\frac{2}{\sqrt{\xi-\alpha}} < \frac{\sqrt{8}}{\sqrt{\xi+M}} \le \frac{\sqrt{8}}{\sqrt{\xi}}$$

since $M \ge 0$, which yields the assertion of Lemma 1. If $\beta, \gamma \in \mathbb{C}\backslash\mathbb{R}$ but $\beta + \gamma = \beta + \overline{\beta} < 2\alpha$, the same conclusion holds since again $\xi/2 > \alpha + M/2$ by (13) and (33).

2. Suppose now that $\beta, \gamma \in \mathbb{C}\backslash\mathbb{R}$ and $\beta + \gamma = \beta + \overline{\beta} \ge 2\alpha$. Then $\beta_1 + \overline{\beta}_1 = 2\alpha - \beta - \overline{\beta} \le 0$, hence $z \ge z + (\beta_1 + \overline{\beta}_1)/2$ and furthermore,

$$\begin{aligned}(z+\beta_1)(z+\overline{\beta}_1) &= z^2 + (\beta_1 + \overline{\beta}_1)z + \beta_1\overline{\beta}_1 \\ &= \left(z + \frac{\beta_1 + \overline{\beta}_1}{2}\right)^2 - \left(\frac{\beta_1 - \overline{\beta}_1}{2}\right)^2 > \left(z + \frac{\beta_1 + \overline{\beta}_1}{2}\right)^2.\end{aligned}$$

Altogether, for $z > 0$ ($\Leftrightarrow x > \alpha$), this leads to the inequality

$$r(z) = z(z+\beta_1)(z+\gamma_1) > \left(z + \frac{\beta_1 + \overline{\beta}_1}{2}\right)^3.$$

The integral (34) can therefore be estimated as follows:

$$\int_{\xi-\alpha}^{\infty} \frac{dz}{\sqrt{r(z)}} < \int_{\xi-\alpha}^{\infty} \frac{dz}{(z + (\beta_1 + \overline{\beta}_1)/2)^{3/2}} = \frac{2}{\sqrt{\xi - \alpha + (\beta_1 + \overline{\beta}_1)/2}}.$$

But in this case, since by (13) and (33),

$$\frac{1}{2}\xi > \frac{\beta + \overline{\beta}}{2} + \frac{M}{2} = \alpha - \frac{\beta_1 + \overline{\beta}_1}{2} + \frac{M}{2},$$

we infer that

$$\frac{2}{\sqrt{\xi-\alpha+(\beta_1+\overline{\beta}_1)/2}} < \frac{\sqrt{8}}{\sqrt{\xi+M}} \le \frac{\sqrt{8}}{\sqrt{\xi}}$$

as before, and this completes the proof of Lemma 1.

P r o o f o f L e m m a 2. By Lemma 2.2 of [PdW], the largest solution $x_0 \in \mathbb{R}$ of the equation $x = \varrho + \sigma \log^\delta x$ satisfies

$$x_0 < 2^\delta(\varrho^{1/\delta} + \sigma^{1/\delta}\log(\sigma\delta^\delta))^\delta.$$

Since $\varrho$ and $\sigma$ are at least 1, we have

$$\varrho^{1/\delta} + \sigma^{1/\delta}\log(\sigma\delta^\delta) \le 2\varrho^{1/\delta}\sigma^{1/\delta}\log(\sigma\delta^\delta),$$

and this implies the asserted inequality.

In the Proposition of Section 3, we need to determine the numbers $V_i \in \mathbb{R}$ in accordance with the conditions (21). This requires the calculation of the elliptic logarithms $u_i$ of the points $P_i \in E(\mathbb{Q})$ and of the real and complex period $\omega_1$ and $\omega_2$, respectively, thus giving $\tau = \omega_2/\omega_1$. To calculate $\omega_1$ and $\omega_2$, we choose for our elliptic curve the above equation

$$v^2 = r(z) = z(z+\beta_1)(z+\gamma_1)$$

and apply the method of arithmetic-geometric mean of Gauss as described by Grayson [Gr]. For the computation of the elliptic logarithms $u_i$ of the points $P_i$ $(1 \le i \le r)$ we use the fast-converging series given by Zagier [Za], formula (10). Of course, the Néron–Tate height of the basis points $P_1, \dots, P_r$ of $E(\mathbb{Q})$, also required in (21), is calculated by the well-known procedure already used in [GZ].

**6. Reduction of the initial bound.** The upper bound for $N$ obtained in the Theorem is in general too large for computing all integral points on our elliptic curve $E$ over $\mathbb{Q}$. However, by numerical diophantine approximation techniques the bound can be considerably reduced. In this way it is eventually possible to solve the elliptic equation in rational integers. The inequality

$$\left|n_0' + \sum_{i=1}^{r} n_i' u_i\right| < gc_1' \exp\{-\lambda_1 N^2\} \tag{35}$$

obtained in the Proposition for $u' = gu$ by virtue of (16′) and (18′), together with the inequality

$$N \le N_2$$

established in the Theorem may be regarded as a homogeneous diophantine approximation problem. Analogous inequalities occur in the resolution of exponential diophantine equations, and methods for solving them have

been studied by de Weger [dW]. We remark that in the applications mentioned above inhomogeneous diophantine approximation problems had to be solved. In the present situation, however, by Mazur's theorem on the torsion, it is more appropriate to utilize homogeneous diophantine approximation techniques. Actually, this is true only if the group of rational points $E(\mathbb{Q})$ is torsion-free or if the upper bound $N_2$ for the coefficients of the basis points is large.

In the sequel, we are going to give an outline of de Weger's method [dW] applied to the present situation. Let $C_0$ be a suitable positive integer and $\Gamma$ be the lattice spanned by the rows of the $(r+1)\times(r+1)$ matrix

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ & & \ddots & & \\ 0 & \dots & 0 & 1 & 0 \\ \lfloor C_0 u_1 \rfloor & \dots & \lfloor C_0 u_{r-1} \rfloor & \lfloor C_0 u_r \rfloor & C_0 \end{pmatrix}.$$

Denote by $l(\Gamma)$ the Euclidean length of the shortest non-zero vector of $\Gamma$. By Lemma 3.7 of [dW], we conclude that, if $\widetilde{N}$ is a positive integer such that

$$l(\Gamma) \geq \sqrt{r^2+5r+4}\, g \widetilde{N},$$

then (35) cannot hold for an $N$ within the range (cf. [dW], Lemma 3.7, (3.22))

$$\sqrt{\frac{1}{\lambda_1}\log\frac{\sqrt{2}\sqrt[3]{4}C_0}{\omega_1 \widetilde{N}}} < N \leq \widetilde{N}. \tag{36}$$

To find a suitable $\widetilde{N}$, one chooses $C_0$ in the order of magnitude of $N_2^{r+1}$ and computes the LLL-reduced basis $\underline{b}_1, \dots, \underline{b}_{r+1}$ of $\Gamma$ (see [LLL]). By Proposition (1.11) of [LLL], we have $l(\Gamma) \geq 2^{-r/2}\|\underline{b}_1\|$, where $\|\underline{b}_1\|$ is the Euclidean length of the vector $\underline{b}_1$. Now we take

$$\widetilde{N} := 2^{-r/2}\|\underline{b}_1\|\big(\sqrt{r^2+5r+4}\, g\big)^{-1}.$$

If $\widetilde{N} \geq N$, we obtain the estimate

$$N \leq \sqrt{\frac{1}{\lambda_1}\log\frac{\sqrt{2}\sqrt[3]{4}C_0}{\omega_1 \widetilde{N}}}.$$

This bound for $N$ is then taken as the new quantity $\widetilde{N}$ and the whole process is iterated until the upper bound cannot be reduced any further.

Let $N_1'$ be the result of the last iteration. In the range we are left with after the reductions, i.e. for the vectors $(n_0, \dots, n_r) \in \mathbb{Z}^{r+1}$ such that $N = \max_{1\leq i\leq r}\{|n_i|\} \leq N_1'$, we now test all points $n_1P_1 + \dots + n_rP_r + P_{r+1}$ in (2) for integrality.

All procedures used in our calculations are part of the computer algebra system SIMATH (see [SM]). It is planned to incorporate in SIMATH the whole algorithm for calculating integral points on elliptic curves over the rationals ([1]).

## 7. Examples

EXAMPLE 1: $y^2 = x^3 - 1642032x + 628747920$.

We take the elliptic curve from Mestre [Me],

$$y^2 + 351y = x^3 - 63x^2 + 56x + 22$$

of rank $r = 6$ over $\mathbb{Q}$ and consider the quasiminimal model in short Weierstrass form

$$E: \quad y^2 = x^3 - 1642032x + 628747920$$

with discriminant

$$\Delta = 112571102923779428352 = 2^{12} \cdot 3^{12} \cdot 51714450757,$$

modular invariant

$$j = \frac{j_1}{j_2} = \frac{224933197418496}{51714450757}$$

and "height" of $E$

$$\mu_\infty = \log \max\{|a|^{1/2}, |b|^{1/3}\} = 7.1557225286.$$

$E$ has trivial torsion group $E_{\mathrm{tors}}(\mathbb{Q}) = \{\mathcal{O}\}$, so that we take $g = 1$.

The six points listed below form a basis of the Mordell–Weil group $E(\mathbb{Q})$. We also display their canonical height $\widehat{h}$:

$$\begin{aligned}
P_1 &= (432, 108), & \widehat{h}(P_1) &= 3.3637106425,\\
P_2 &= (396, 6372), & \widehat{h}(P_2) &= 3.3888408529,\\
P_3 &= (360, 9180), & \widehat{h}(P_3) &= 3.4129391620,\\
P_4 &= (1044, 7236), & \widehat{h}(P_4) &= 3.5302197591,\\
P_5 &= (108, 21276), & \widehat{h}(P_5) &= 3.5591324536,\\
P_6 &= (36, 23868), & \widehat{h}(P_6) &= 3.5952919707.
\end{aligned}$$

The symmetric matrix of the bilinear form associated with the quadratic

([1]) After we had finished writing this paper, we learned that in a lecture, delivered in October 1993 at Oberwolfach, Tzanakis had also reported on an algorithm for computing integral points on elliptic curves by means of elliptic logarithms. After we had submitted this manuscript, we received the preprint [ST] of Stroeker and Tzanakis.

form $\widehat{h}$ on $E(\mathbb{Q})$ with respect to the points $P_1, \ldots, P_6$ is

$$A = \begin{pmatrix} 3.36371 & -0.01723 & -0.35870 & 1.41713 & 1.09316 & -1.20380 \\ -0.01723 & 3.38884 & -0.87466 & 0.78051 & 0.71168 & 0.86176 \\ -0.35870 & -0.87466 & 3.41294 & 1.51057 & -1.45781 & 0.67460 \\ 1.41713 & 0.78051 & 1.51057 & 3.53022 & -0.87592 & -0.21851 \\ 1.09316 & 0.71168 & -1.45781 & -0.87592 & 3.55913 & -1.76537 \\ -1.20380 & 0.86176 & 0.67460 & -0.21851 & -1.76537 & 3.59529 \end{pmatrix}.$$

The matrix $A$ has the characteristic polynomial

$$\chi_A(x) = x^6 - 20.85013503x^5 + 164.9142957x^4 - 618.6663540x^3 + 1125.293711x^2 - 906.8522386x + 226.2807738.$$

The eigenvalues of $A$ are

$$\begin{aligned} \lambda_1 &= 0.4323724011, & \lambda_4 &= 4.3502898759, \\ \lambda_2 &= 1.5647578466, & \lambda_5 &= 5.5014070699, \\ \lambda_3 &= 1.9944764779, & \lambda_6 &= 7.0068311531, \end{aligned}$$

of which $\lambda_1$ is needed in (5).

The real period given by (10) is

$$\omega_1 = 1.0582679843$$

and the complex period is

$$\omega_2 = 0.4067231150i$$

so that

$$\tau = \frac{\omega_2}{\omega_1} = 0.3843290367i.$$

Hence the constant in (17) becomes $c_1' = 4.2426382163$ thus yielding the constant in (29)

$$c_1 = \max\left\{\frac{\log(1 \cdot c_1')}{\lambda_1},\ 1\right\} = 1.4451852966.$$

In (21) we need the elliptic logarithms of the basis points $P_1, \ldots, P_6$:

$$\begin{aligned} u_1 &= 0.0011316844, & u_4 &= 0.4447562185, \\ u_2 &= 0.0649588423, & u_5 &= 0.1867017663, \\ u_3 &= 0.0912606341, & u_6 &= 0.2047900792, \end{aligned}$$

and the quantity from (20),

$$h = \log \max\{4|aj_2|, 4|bj_2|, |j_1|, |j_2|\} = 46.3145384235,$$

whence

$$\max\left\{\widehat{h}(P_i), h, \frac{3\pi u_i^2}{\omega_1^2 \mathrm{Im}(\tau)}\right\} = h \quad \text{for } i = 1, \ldots, 6.$$

Therefore we may choose

$$V = V_i = e^h = 130061413389624701760 \quad (i = 1, \dots, 6)$$

in accordance with (21) and (22). It turns out that (22) is automatically satisfied if we take $B = \frac{7}{2}N$ as required by (24). The constant $C$ in (25) is $C \sim 7 \cdot 10^{213}$ and therefore, the constant $c_2$ in (29) becomes

$$c_2 = \max\left\{\frac{C}{\lambda_1}, 10^9\right\}\left(\frac{h}{2}\right)^{r+1}\prod_{i=1}^{r}\log V_i = \frac{C}{2^{r+1}\lambda_1}h^{2r+1} \sim 2.5 \cdot 10^{233}.$$

Finally, in (31) we get

$$N_1 = 1.1 \cdot 10^{126}$$

and the Theorem shows that

$$N \le N_2 = \max\{N_1, 2e^h/7\} = N_1.$$

Now we apply de Weger reduction to the $7 \times 7$ matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \lfloor C_0u_1\rfloor & \lfloor C_0u_2\rfloor & \lfloor C_0u_3\rfloor & \lfloor C_0u_4\rfloor & \lfloor C_0u_5\rfloor & \lfloor C_0u_6\rfloor & C_0 \end{pmatrix}$$

starting with the value $C_0 = 10^{890} \sim N_1^7$. After the first reduction, the length of the shortest vector $\underline{b}_1$ of the lattice $\Gamma$ is $\|\underline{b}_1\| \ge 1.16 \cdot 10^{127}$ and we obtain the new upper bound $N \le 64$.

In a second application of the de Weger reduction we choose the starting value $C_0 = 2 \cdot 10^{21}$ to ensure that (36) is satisfied. It reduces the length of the shortest vector $\underline{b}_1$ of the lattice to $\|\underline{b}_1\| \ge 114.7$ and yields the bound $N \le 10$.

A third reduction leads to the same upper bound for $N$. By using LLL-reduction on vectors of real numbers instead of integral numbers as in de Weger's method, the upper bound is improved to $N \le 8$. This improvement is achieved since, by passing to the real case, one obtains a sharper estimate for the shortest vector in the lattice $\Gamma$.

Our task is therefore to test for integrality all the points

$$P = n_1P_1 + n_2P_2 + n_3P_3 + n_4P_4 + n_5P_5 + n_6P_6$$

such that $|n_i| \le N \le 8$ $(1 \le i \le 6)$. It then remains to test the points $P = (\xi, \eta) \in E(\mathbb{Q})$ such that

$$\xi \in \mathbb{Z} \quad \text{and} \quad 0 \le \log|\xi| \le \mu_\infty = 7.1557225286$$

in order to take care of the case in which (9′) rather than (9) is valid. In addition, we also have to search for integral points on the compact component of $E/\mathbb{Q}$, namely the points $P$ such that

$$-1441.589746 \sim \beta \le \xi \le \gamma \sim 432.0107786$$

in accordance with the Remark following Lemma 1. By this extra search, however, we did not find any new points.

Altogether we obtained the 70 integral points (and their additive inverses, of course) on $E$ over $\mathbb{Q}$ displayed in Table 1. They constitute the complete set of integral points in $E(\mathbb{Q})$.

R e m a r k. Table 1 shows that the actual bound for $N$ is 2 rather than 8.

**Table 1**

| No. | $P$ | $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | $n_6$ | $\widehat{h}(P)$ |
|---|---|---|---|---|---|---|---|---|
| 1 | $(-1440, 2700)$ | 0 | −1 | −1 | 1 | 0 | 1 | 4.0860684 |
| 2 | $(-1431, 6939)$ | 0 | 0 | 1 | 0 | 1 | 1 | 5.4701995 |
| 3 | $(-1388, 15292)$ | 1 | 0 | 1 | −1 | −1 | 0 | 6.2707058 |
| 4 | $(-1332, 21276)$ | −1 | 0 | 0 | 1 | 0 | 0 | 4.0596804 |
| 5 | $(-1296, 24084)$ | 1 | 1 | 0 | −1 | −1 | 0 | 4.0506693 |
| 6 | $(-1031, 35011)$ | 0 | 2 | 1 | −1 | −1 | −1 | 7.5641857 |
| 7 | $(-999, 35667)$ | 0 | −1 | 0 | 1 | 0 | 0 | 5.3580305 |
| 8 | $(-927, 36801)$ | 0 | 0 | 0 | −1 | −1 | 0 | 5.3375206 |
| 9 | $(-828, 37692)$ | 0 | 0 | −1 | 1 | 0 | 0 | 3.9220270 |
| 10 | $(-648, 37692)$ | 0 | −1 | 0 | 0 | 1 | 1 | 3.8656383 |
| 11 | $(-612, 37476)$ | 1 | 1 | 1 | −1 | −1 | −1 | 3.8537954 |
| 12 | $(-396, 34884)$ | −1 | −1 | −1 | 1 | 0 | 0 | 3.7781382 |
| 13 | $(-332, 33724)$ | −1 | 0 | 1 | 0 | 1 | 0 | 5.9512406 |
| 14 | $(-72, 27324)$ | 0 | 1 | 0 | −1 | −1 | −1 | 3.6459771 |
| 15 | $(36, 23868)$ | 0 | 0 | 0 | 0 | 0 | 1 | 3.5952920 |
| 16 | $(108, 21276)$ | 0 | 0 | 0 | 0 | 1 | 0 | 3.5591325 |
| 17 | $(184, 18244)$ | 1 | 0 | 0 | −1 | −1 | −1 | 5.7158004 |
| 18 | $(297, 12933)$ | −1 | −1 | −1 | 2 | 1 | 1 | 4.8391918 |
| 19 | $(360, 9180)$ | 0 | 0 | 1 | 0 | 0 | 0 | 3.4129392 |
| 20 | $(396, 6372)$ | 0 | 1 | 0 | 0 | 0 | 0 | 3.3888409 |
| 21 | $(412, 4708)$ | 0 | −1 | −1 | 0 | 0 | 1 | 5.5750298 |
| 22 | $(432, 108)$ | 1 | 0 | 0 | 0 | 0 | 0 | 3.3637106 |
| 23 | $(1017, 3267)$ | −1 | −1 | −1 | 1 | 1 | 0 | 4.8913920 |
| 24 | $(1044, 7236)$ | 0 | 0 | 0 | 1 | 0 | 0 | 3.5302198 |
| 25 | $(1048, 7676)$ | 0 | 0 | 1 | −1 | 0 | −1 | 5.7311012 |
| 26 | $(1060, 8900)$ | 0 | 1 | 0 | −1 | −1 | 0 | 5.7419748 |
| 27 | $(1152, 16308)$ | 0 | 0 | 0 | 0 | 1 | 1 | 3.6236835 |
| 28 | $(1192, 19108)$ | −1 | −1 | 0 | 1 | 0 | 0 | 5.8530373 |
| 29 | $(1224, 21276)$ | 1 | 0 | 0 | −1 | −1 | 0 | 3.6806690 |
| 30 | $(1296, 26028)$ | −1 | 0 | −1 | 1 | 0 | 0 | 3.7340954 |
| 31 | $(1441, 35423)$ | −1 | −1 | 0 | 0 | 1 | 1 | 7.4161825 |
| 32 | $(1476, 37692)$ | 0 | 1 | 1 | −1 | −1 | −1 | 3.8548934 |

**Table 1** (cont.)

| No. | $P$ | $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | $n_6$ | $\widehat{h}(P)$ |
|---|---|---|---|---|---|---|---|---|
| 33 | $(1728, 54324)$ | 0 | −1 | −1 | 1 | 0 | 0 | 4.0005237 |
| 34 | $(1836, 61668)$ | 0 | 0 | 1 | 0 | 1 | 0 | 4.0564499 |
| 35 | $(2385, 101385)$ | −1 | 0 | 0 | 1 | 0 | −1 | 5.6843920 |
| 36 | $(2556, 114588)$ | 1 | 1 | 0 | −1 | −1 | −1 | 4.3622713 |
| 37 | $(3132, 161892)$ | 1 | 0 | 0 | 0 | 0 | 1 | 4.5514029 |
| 38 | $(3816, 223452)$ | −1 | 0 | 0 | 0 | 1 | 0 | 4.7365309 |
| 39 | $(4689, 309879)$ | 0 | 0 | −1 | 1 | −1 | 0 | 6.3173694 |
| 40 | $(4860, 327780)$ | 0 | 0 | 0 | −1 | −1 | −1 | 4.9650524 |
| 41 | $(5328, 378324)$ | 0 | 1 | 1 | 0 | 0 | 0 | 5.0524660 |
| 42 | $(6624, 529524)$ | 0 | −1 | 0 | 0 | 0 | 1 | 5.2606033 |
| 43 | $(8296, 746972)$ | 0 | −1 | −1 | 2 | 1 | 1 | 7.6745398 |
| 44 | $(8712, 804708)$ | 0 | −1 | 0 | 0 | 1 | 0 | 5.5246168 |
| 45 | $(10008, 993276)$ | 0 | 0 | −1 | 0 | 0 | 1 | 5.6590325 |
| 46 | $(15084, 1846044)$ | 1 | 0 | 1 | 0 | 0 | 0 | 6.0592576 |
| 47 | $(15849, 1988901)$ | −1 | 0 | 1 | 0 | 0 | 0 | 7.4940421 |
| 48 | $(18856, 2583388)$ | −1 | −1 | −1 | 1 | 0 | −1 | 8.4755779 |
| 49 | $(19548, 2727324)$ | 1 | 1 | 1 | −2 | −1 | 0 | 6.3138077 |
| 50 | $(29448, 5048676)$ | 1 | 1 | 0 | 0 | 0 | 0 | 6.7180976 |
| 51 | $(31572, 5605308)$ | −1 | 1 | 0 | 0 | 0 | 0 | 6.7870054 |
| 52 | $(32356, 5815612)$ | 1 | 1 | 1 | −2 | 0 | −1 | 9.0085106 |
| 53 | $(37332, 7208892)$ | −1 | −2 | −1 | 2 | 1 | 1 | 6.9530002 |
| 54 | $(45328, 9646676)$ | 0 | 0 | 0 | 1 | −1 | −1 | 9.3427541 |
| 55 | $(52056, 11873412)$ | 1 | −1 | −1 | 0 | 0 | 1 | 7.2829869 |
| 56 | $(72864, 19665396)$ | 0 | 1 | 0 | −1 | −2 | −1 | 7.6174453 |
| 57 | $(83988, 24337476)$ | 1 | 0 | 1 | −1 | 1 | 1 | 7.7589192 |
| 58 | $(113233, 38100599)$ | 2 | 2 | 2 | −2 | −1 | −1 | 11.6401838 |
| 59 | $(122544, 42895764)$ | −1 | −1 | −2 | 2 | 1 | 1 | 8.1354623 |
| 60 | $(149260, 57663260)$ | −1 | −1 | −1 | 0 | 1 | 0 | 10.5294159 |
| 61 | $(185868, 80130276)$ | 0 | −1 | 1 | 0 | 0 | 0 | 8.5510941 |
| 62 | $(224712, 106520292)$ | 0 | 1 | 0 | −1 | −1 | −2 | 8.7405633 |
| 63 | $(270108, 140378724)$ | −1 | 0 | 0 | 1 | 2 | 1 | 8.9243130 |
| 64 | $(392985, 246355155)$ | 0 | 0 | 0 | 0 | −1 | 1 | 10.6851654 |
| 65 | $(429129, 281112309)$ | 2 | 0 | 1 | −2 | −1 | 0 | 10.7730789 |
| 66 | $(1149912, 1233095292)$ | 0 | −1 | −2 | 1 | −1 | 0 | 10.3719724 |
| 67 | $(1590228, 2005344324)$ | −2 | −1 | 0 | 2 | 1 | 0 | 10.6960827 |
| 68 | $(4361004, 9107091684)$ | −1 | −2 | −1 | 1 | 2 | 2 | 11.7047719 |
| 69 | $(13895892, 51799986108)$ | 0 | 0 | −1 | 2 | 0 | 1 | 12.8636093 |
| 70 | $(25099236, 125745007932)$ | 2 | 0 | 0 | 0 | 0 | 0 | 13.4548426 |

EXAMPLE 2: $y^2 = x^3 - 203472x + 18487440$.

We take the curve

$$y^2 + 67y = x^3 - 21x^2 - 10x + 30$$

from Mestre [Me] of rank $r = 5$ over $\mathbb{Q}$ and consider the model in short

Weierstrass form

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

The points

$$(72, 2052), \quad (36, 3348), \quad (-36, 5076), \quad (-72, 5724), \quad (396, 108)$$

form a basis of the Mordell–Weil group $E(\mathbb{Q})$.

Starting with $N_1 = 1.3 \cdot 10^{96}$ and $C_0 = 10^{600}$, we obtain, after the first reduction, $N \leq 37$, and after the second, $N \leq 6$. A third reduction yields the same upper bound $N \leq 6$. Again, real LLL-reduction improves the upper bound to $N \leq 5$.

We list the first coordinates $\xi$ of the $(2\times)$ 48 integral points on the short Weierstrass model of $E$ over $\mathbb{Q}$ which constitute the set of all integral points in $E(\mathbb{Q})$.

**Table 2**

$-488,\ -468,\ -432,\ -423,\ -351,\ -279,\ -216,\ -180,\ -72,$

$-36,\ 4,\ 36,\ 72,\ 81,\ 88,\ 396,\ 432,\ 433,\ 468,\ 496,\ 520,\ 576,$

$720,\ 748,\ 1188,\ 1404,\ 1944,\ 2448,\ 2916,\ 3204,\ 3897,\ 4320,$

$7092,\ 7272,\ 8388,\ 13689,\ 14176,\ 17452,\ 22392,\ 53856,\ 55656,$

$90108,\ 157212,\ 163872,\ 1348776,\ 1526904,\ 45548136,\ 372941316$

R e m a r k. Mestre [Me] computes only the $(2\times)$ 31 integral points $(\xi, \eta)$ with $\xi < 10^6$ on the model in long Weierstrass form

$$y^2 + 67y = x^3 - 21x^2 - 10x + 30.$$

In addition to all the points he found our algorithm turned up two more points on his model, namely

$$(1265233, -1423154899) \quad \text{and} \quad (10359488, -33343178529).$$

Example 3: $y^2 = x^3 - 879984x + 319138704$.

We take the curve

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

of rank $r = 5$ over $\mathbb{Q}$. The points

$$(540, 1188),\ (576, 1836),\ (468, 3132),\ (612, 3132),\ (432, 4428)$$

form a basis of the Mordell–Weil group $E(\mathbb{Q})$.

Starting with $N_1 = 2 \cdot 10^{96}$ and $C_0 = 10^{600}$, we obtain, after the first reduction, $N \leq 40$, and after the second, $N \leq 7$. A third reduction yields no improvement. As above, by using real LLL-reduction, the upper bound can be improved to $N \leq 6$.

We list the first coordinates $\xi$ of the $(2\times)$ 54 integral points on $E$ over $\mathbb{Q}$ which constitute the set of all integral points in $E(\mathbb{Q})$.

**Table 3**

$-1080,\ -900,\ -864,\ -792,\ -764,\ -684,\ -620,\ -423,\ -279,\ -72,$
$36,\ 108,\ 172,\ 376,\ 396,\ 432,\ 468,\ 513,\ 520,\ 540,\ 576,\ 585,\ 612,\ 673,$
$720,\ 792,\ 972,\ 1072,\ 1368,\ 1732,\ 2113,\ 2385,\ 2448,\ 2592,\ 3060,\ 3537,$
$4680,\ 5940,\ 8668,\ 9972,\ 14265,\ 17856,\ 36828,\ 43200,\ 65052,\ 78696,$
$114280,\ 155356,\ 193320,\ 196992,\ 368892,\ 1260648,\ 2717460,\ 2204663452$

## References


[B] A. Baker, *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. 43 (1968), 1–9.

[D] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, manuscript, Paris, 1993.

[F] G. Frey, *L-series of elliptic curves*: *results*, *conjectures and consequences*, in: Proc. Ramanujan Centenn. Internat. Conf., Annamalainagar, December 1987, 31–43.

[GPP] I. Gaàl, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields II*, J. Number Theory 38 (1991), 35–51.

[GSch] I. Gaàl and N. Schulte, *Computing all power integral bases of cubic number fields II*, Math. Comp. 53 (1989), 689–696.

[G] F. R. Gantmacher, *The Theory of Matrices I*, Chelsea, New York, N.Y., 1977.

[GZ] J. Gebel and H. G. Zimmer, *Computing the Mordell–Weil group of an elliptic curve over* $\mathbb{Q}$, in: Elliptic Curves and Related Topics, H. Kisilevsky and M. Ram Murty (eds.), CRM Proceedings and Lecture Notes, Amer. Math. Soc., Providence, RI, 1994, 61–83.

[Gr] D. R. Grayson, *The arithmetic-geometric mean*, Arch. Math. (Basel) 52 (1989), 507–512.

[HSi] A. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450.

[L1] S. Lang, *Diophantine approximation on toruses*, Amer. J. Math. 86 (1964), 521–533.

[L2] —, *Elliptic Functions*, Addison-Wesley, Reading, 1973.

[L3] —, *Elliptic Curves*; *Diophantine Analysis*, Grundlehren Math. Wiss. 231, Springer, Berlin, 1978.

[L4] —, *Conjectured diophantine estimates on elliptic curves*, in: Progr. Math. 35, Birkhäuser, Basel, 1983, 155–171.

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

[M] Yu. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys 26 (6) (1971), 7–78.

[Mz] B. Mazur, *Rational points on modular curves*, in: Modular Functions of One Variable V, Lecture Notes in Math. 601, Springer, Berlin, 1977, 107–148.

[Me] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. 58 (1986), 209–232.

[PS] A. Pethő und R. Schulenberg, *Effektives Lösen von Thue Gleichungen*, Publ. Math. Debrecen 34 (1987), 189–196.

[PdW] A. Pethő and B. M. M. de Weger, *Product of prime powers in binary recurrence sequences*, *Part I*: *The hyperbolic case*, *with an application to the generalized Ramanujan–Nagell equation*, Math. Comp. 47 (1986), 713–727.

[Sch] W. Schmidt, *Integer points on curves of genus* 1, Compositio Math. 81 (1992), 33–59.

[S] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. (1929), 1–41.

[Si1] J. H. Silverman, *A quantitative version of Siegel's theorem*, J. Reine Angew. Math. 378 (1981), 60–100.

[Si2] —, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723–743.

[SM] *SIMATH*, Manual, Saarbrücken, 1993.

[St] R. P. Steiner, *On Mordell's equation* $y^2 - k = x^3$. *A problem of Stolarsky*, Math. Comp. 46 (1986), 703–714.

[ST] R. J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. 67 (1994), 177–196.

[TdW1] N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory 31 (1989), 99–132.

[TdW2] —, —, *How to explicitly solve a Thue–Mahler equation*, Compositio Math. 84 (1992), 223–288.

[dW] B. M. M. de Weger, *Algorithms for diophantine equations*, Ph.D. Thesis, Centrum voor Wiskunde en Informatica, Amsterdam, 1987.

[Za] D. Zagier, *Large integral points on elliptic curves*, Math. Comp. 48 (1987), 425–436.

[Zs] H. Zassenhaus, *On Hensel factorization*, *I*, J. Number Theory 1 (1969), 291–311.

[Zi1] H. G. Zimmer, *On the difference between the Weil height and the Néron–Tate height*, Math. Z. 147 (1976), 35–51.

[Zi2] —, *On Manin's conditional algorithm*, Bull. Soc. Math. France Mém. 49–50 (1977), 211–224.

[Zi3] —, *Generalization of Manin's conditional algorithm*, in: SYMSAC 76, Proc. ACM Sympos. Symbolic Alg. Comp., Yorktown Heights, N.Y., 1976, 285–299.

[Zi4] —, *Computational aspects of the theory of elliptic curves*, in: Number Theory and Applications, R. A. Mollin (ed.), Kluwer, 1989, 279–324.

[Zi5] —, *A limit formula for the canonical height of an elliptic curve and its application to height computations*, in: Number Theory, R. A. Mollin (ed.), W. de Gruyter, Berlin, 1990, 641–659.

FACHBEREICH 9 MATHEMATIK
UNIVERSITÄT DES SAARLANDES
D-66041 SAARBRÜCKEN, GERMANY

LABORATORY FOR INFORMATICS
UNIVERSITY MEDICAL SCHOOL
NAGYERDEI KRT. 98
H-4028 DEBRECEN, HUNGARY

*Received on 9.12.1993* (2539)