Computing Integral Points on Elliptic Curves

J. Gebel, A. Pethö and H. G. Zimmer

November 28, 2009

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 Demjanenko [L3] 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 E 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], 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 exhibited by W. Schmidt [Sch, Th. 2]. However, the bounds are rather large and therefore can be used only for soloving some particular equations (see [TdW], [St]) or for treating a special model of elliptic curves, namely Thue curves of degree 3 (see [GSch]).

The Siegel-Baker method for the computation for integer points on elliptic curves E over $\mathbb{K} = \mathbb{Q}$ requires some detailed information about certain quartic number fields. Computing these fields often represents a hard problem and this approach does not seem to be adaquate. That is why in general all these results cannot be used for the actual calculation of all integral points on an elliptic curve E over $\mathbb{Q}$. another method was suggested by Lang [L1], [L3]. His idea was further developed by Zagier [Za].

We shall work out the Lang-Zagier algorithm for the determination of all integral points on elliptic curves E over $\mathbb{Q}$ employing elliptic logarithms. The algorithm requires the knowledge of abasis 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 method, it thus appears to be more natural and adaquate to 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 of elliptic curves of ranks up to at least six.

As mentioned above, or 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 developed by the first and the last author [GZ]. It is based on ideas of Manin [M] and depends on the truth of the conjectures of Birch and Swinnerton-Dyer (see e.g. [F]). We are planning to make it independent of this conjecture. The second ingredient is an explicit lower bound for linear forms in elliptic logarithms of algebraic numbers. It was only recently that S. David [D] established such an explicit bound, thus proving a 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], [TdW], [GPP]). The reduction procedure, based on numerical diophantine approximation techniques, is the third important ingredient 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*

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

with integral rational coefficients a, b. 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 $P = (\frac{\xi}{\zeta^2},\, \frac{\eta}{\zeta^3}) \in E(\mathbb{Q})$, where $\xi,\ \eta,\ \zeta \in \mathbb{Z}$ and $\gcd(\xi,\, \zeta) = \gcd(\eta,\, \zeta) = 1$, the *ordinary height* or *Weil height* is

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

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

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

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

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

By embedding $\overline{E}(\mathbb{Q})$ into the r-dimensional real space $\mathcal{E}(\mathbb{R}) := E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$, it is clear that $\hat{h}$ extends to a positive definite quadratic form $\hat{h}$ 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 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 an arbitrary rational point $P \in E(\mathbb{Q})$ has a unique representation of the form

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

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

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

$$P' = \sum_{i=1}^{r} n_i' P_i, \qquad (n_i' = g \cdot n_i). \tag{1'}$$

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

$$g \leq 12. \tag{2}$$

Of course, in practise 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

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

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

$$N := \max_{1\leq i\leq r} \{|n_i|\}. \tag{3}$$

Let us look at the representation (1) modulo torsion, viz.

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

and consider the embedding

$$\overline{E}(\mathbb{Q}) \hookrightarrow \mathcal{E}(\mathbb{R}) \cong \mathbb{R}^r.$$

Since $\hat{h}$ 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)

$$\hat{h}(P) \geq \lambda_1 \cdot N^2 \tag{4}$$

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 $\hat{h}$ and the given basis $P_1, \ldots, P_r$ of $E(\mathbb{Q})$.

Next we are going to replace in (4) the canonical height $\hat{h}$ by a modified ordinary height d to be used in place of h. This is carried out by means of an estimate between $\hat{h}$ and d on $E(\mathbb{Q})$. The modified ordinary height of a point $P = (\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3}) \in E(\mathbb{Q})$ is defined as (cf. [Zi1], [Zi5])

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

with the "height" of E

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

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

$$-\tfrac{2}{3}\alpha \leq d(P) - \hat{h}(P) \leq \tfrac{3}{2}\mu_\infty + \tfrac{5}{3}\alpha, \tag{5}$$

where $\alpha = \log 2$. In fact on combining the height estimates obtained in [Zi2], [Zi3] with those from [Zi5], one ends up with the slightly stronger estimates

$$-\tfrac{7}{12}\alpha \leq d(P) - \hat{h}(P) \leq \tfrac{2}{3}\mu_\infty + \tfrac{19}{12}\alpha. \tag{5$'$}$$

For the sake of simplicity, however, we shall use (5) rather than (5$'$). (Note that the height d in [Zi2], [Zi3] differs from the above-defined d by a factor of 3.)

From (5) we derive

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

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

$$\tfrac{1}{2}\log|\xi| \geq \hat{h}(P) - \tfrac{3}{2}\log 2. \tag{6}$$

Combining (4) and (6) yields

$$\tfrac{1}{2}\log|\xi| \geq \lambda_1 N^2 - \tfrac{2}{3}\log 2. \tag{7}$$

We remark that if μ_∞ is large, e.g. $\exp(\mu_\infty) > 10^6$, and if $0 \leq \log|\xi| \leq \mu_\infty$, we must refine the estimates (5) - (7) as follows. It is easy to see that, for integral points $P \in E(\mathbb{Q})$, we have

$$0 \leq d(P) - h(P) \leq \tfrac{1}{2}\mu_\infty.$$

Combining these inequalities with (5) yields

$$-\tfrac{2}{3}\alpha - \tfrac{1}{2}\mu_\infty \leq h(P) - \hat{h}(P) \leq \tfrac{3}{2}\mu_\infty + \tfrac{5}{3}\alpha. \tag{5''}$$

From (5″) we get the lower estimate

$$h(P) \geq \hat{h}(P) - \tfrac{2}{3}\alpha - \tfrac{1}{2}\mu_\infty$$

and hence

$$\tfrac{1}{2}\log|\xi| \geq \hat{h}(P) - \tfrac{2}{3}\log 2 - \tfrac{1}{2}\mu_\infty. \tag{6'}$$

Therefore, in the case of $0 \leq \log|\xi| \leq \mu_\infty$, (7) is to be replaced by the weaker inequality

$$\tfrac{1}{2}\log|\xi| \geq \lambda_1 N^2 - \tfrac{2}{3}\log 2 - \tfrac{1}{2}\mu_\infty. \tag{7'}$$

This case requires an extra search procedure.

We confine ourselves to explaining the search procedure for *large* integral points $P = (\xi,\ \eta) \in E(\mathbb{Q})$ for which therefore the stronger bound in (7) may be taken.

3 Elliptic logarithms

The next step consists in inserting in (7) the elliptic logarithm of P. To this end, we use the Weierstrass-parametrization of our elliptic curve E (see, e.g., [L2]). There exists a lattice $\Omega \subseteq \mathbb{C}$ such that the group of complex points is

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

where $\Omega = <\omega_1, \omega_2>$ is generated by two *fundamental periods* ω_1 and ω_2 of which ω_1 is real and ω_2 complex. We put $\tau = \frac{\omega_2}{\omega_1}$ and assume without loss of generality that $\mathrm{Im}\,(\tau) > 0$. The above isomorphism is defined by Weierstrass' $\wp$-function with respect to Ω and its derivative $\wp'$ according to the assignment

$$P = (\wp(u),\ \wp'(u)) \longleftarrow\!\shortmid u \mod \Omega,$$

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

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

Let $\alpha \in \mathbb{R}$ be the largest real root of the right hand side of the Weierstrass equation, i.e. of

$$p(x) := x^3 + ax + b. \tag{8}$$

Then the real period ω_1 of E is (cf. [Za])

$$\omega_1 = 2 \int_{\alpha}^{\infty} \frac{dx}{\sqrt{x^3 + ax + b}}. \tag{9}$$

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

$$u \equiv \frac{1}{\omega_1} \int_{\xi}^{\infty} \frac{dx}{\sqrt{x^3 + ax + b}} \pmod{\mathbb{Z}}. \tag{10}$$

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

$$M := \left\{ \begin{array}{ll} 0 & \text{if } \alpha \geq 0 \\ \dfrac{\exp(\mu_\infty)}{\sqrt[3]{2} - 1} & \text{if } \alpha < 0 \end{array} \right\} \tag{11}$$

and choose a real number

$$\xi_0 \geq \left\{ \begin{array}{ll} 2\alpha + M & \text{if } \beta, \gamma \in \mathbb{R} \\ 2 \max\left\{\alpha, \dfrac{\beta + \gamma}{2}\right\} + M & \text{if } \beta, \gamma \in \mathbb{C}\backslash\mathbb{R} \end{array} \right\}. \tag{12}$$

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

$$\int_{\xi}^{\infty} \frac{dx}{\sqrt{x^3 + ax + b}} < \frac{\sqrt{8}}{\sqrt{\xi}}. \tag{13}$$

Remark If $\xi < 0$ it must be bounded in absolute value since otherwise $p(\xi)$ could not be a square. This case must be included in the extra search procedure.

We shall prove this lemma later and proceed instead in our task of estimating elliptic logarithms. Normalizing the value of u in (10) to

$$0 < |u| \leq \frac{1}{2},$$

we obtain from (10) and (13) the estimate

$$|u| < \frac{\sqrt{8}}{\omega_1} \cdot \frac{1}{\sqrt{|\xi|}}. \tag{14}$$

We shall work with (7) rather than with (7′) remembering that in (7′) we may drop the term $-\frac{1}{2}\mu_\infty$ if $|\xi|$ is sufficiently large, i.e. if $\log|\xi| > \mu_\infty$. On combining (7) and (14), we arrive at

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

Exponentiating leads to

$$|u| < \exp\{-\lambda_1 N^2 + c_1'\} \tag{15}$$

for

$$c_1' := \log\frac{\sqrt{8}\cdot\sqrt[3]{4}}{\omega_1}. \tag{16}$$

Now we are going to utilize the crucial Theorem 2.1 of David ([D]). Written in terms of elliptic logarithms, equation (1) 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 $P_{r+1} \in E_{\mathrm{tors}}(\mathbb{Q})$ and, for $1 \leq i \leq r$, the u_i are the elliptic logarithms of the basis points $P_i \in E(\mathbb{Q})$. Rewritten as an equality, this congruence becomes

$$u = n_0 + \sum_{i=1}^{r} n_i u_i + u_{r+1} \tag{17}$$

for some integer $n_0 \in \mathbb{Z}$. If we replace (1) by (1′) we obtain for the elliptic logarithm $u' = gu$ of the point $P' = gP \in E(\mathbb{Q})$ the representation

$$u' = n_0' + \sum_{i=1}^{r} n_i' u_i + u_{r+1} \qquad (n_i' = g n_i \in \mathbb{Z}) \tag{17′}$$

which we shall use instead of (17). Of course, (15) is then to be replaced by

$$|u'| < \exp\{-\lambda_1 N^2 + c_1' + \log g\} \tag{15′}$$

Here again we assume the elliptic logarithms normalized to

$$0 < |u_i| \leq \tfrac{1}{2} \quad (1 \leq i \leq r). \tag{18}$$

Since David works with the classical Weierstrass form

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

we have to 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 infinity, and $|\ |_p$ denotes the normalized multiplicative p-adic valuation and $|\ |$ the ordinary absolute value of $\mathbb{Q}$. On writing the modular invariant in simplest fraction representation $j = \frac{j_1}{j_2}$ for $j_1,\, j_2 \in \mathbb{Z}$ such that $\gcd(j_1,\, j_2) = 1$ and using the sum formula

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

we obtain for h the expression

$$\begin{aligned} h &= h(1,\, -4a,\, -4b,\, \frac{j_1}{j_2}) \\ &= \sum_p \max\{0,\, \log |4a|_p,\, \log |4b|_p,\, \log |j_1|_p - \log |j_2|_p\} \\ &\qquad + \max\{0,\, \log |4a|,\, \log |4b|,\, \log |j_1| - \log |j_2|\} \\ &= -\sum_p \min\{-\log |j_2|_p,\, -\log |4aj_2|_p,\, -\log |4bj_2|_p,\, -\log |j_1|_p\} \\ &\qquad + \log \max\{4|aj_2|,\, 4|bj_2|,\, |j_1|,\, |j_2|\} \\ &= \log \max\{4|aj_2|,\, 4|bj_2|,\, |j_1|,\, |j_2|\} \end{aligned} \tag{19}$$

since a, b, j_1, j_2 are integers and j_1, j_2 are relatively prime. Therefore, we take the latter expression as the value h in David's Theorem 2.1. Furthermore, we

choose $D := 1$ and real numbers $V_1, \ldots, V_r$ and B such that, in accordance with (1) and (1′),

$$\log V_i \geq \max\Big\{\hat{h}(P_i),\, h,\, \frac{3\pi|u_i|^2}{\omega_1^2 \mathrm{Im}\,(\tau)}\Big\} \quad \text{for } 1 \leq i \leq r \tag{20}$$

and, a fortiori,

$$B \geq \max_{1\leq i\leq r}\{V_i\}. \tag{21}$$

It turns out to be necessary to impose another condition on B. To this end, note that by the definition (3) of N, we have for the coefficients n_i' in (1′) the estimates

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

On the other hand, the integer n_0' in (17) can be estimated as follows: Applying (15) to $u' = gu$ we get from (17′)

$$\Big|n_0' + \sum_{i=1}^{r} n_i' u_i\Big| < \exp\{-\lambda_1 N^2 + c_1' + \log g\},$$

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

$$N \geq \sqrt{\frac{\log(2g) + c_1'}{\lambda_1}}. \tag{22}$$

Hence, we obtain

$$\begin{aligned}
|n_0'| &= \Big|n_0' + \sum_{i=1}^{r} n_i' u_i - \Big(\sum_{i=1}^{r} n_i' u_i)\Big| \\
&\leq \Big|n_0' + \sum_{i=1}^{r} n_i' u_i\Big| + \Big|\sum_{i=1}^{r} n_i' u_i\Big| \\
&\leq \tfrac{1}{2} + \sum_{i=1}^{r} |n_i'|\,|u_i| \\
&\leq \tfrac{1}{2} + \tfrac{r}{2} gN \;\leq\; \tfrac{r+1}{2} gN
\end{aligned}$$

by the normalization (18) of the u_i.

Therefore, assuming (22) and $N > e^e$, we choose

$$B := \frac{r+1}{2} gN, \tag{23}$$

keeping in mind that condition (21) must be fulfilled, too.

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

$$C := 1.1 \cdot 10^9 \cdot 10^{7r} \cdot \Big(\frac{2}{e}\Big)^{2r^2} \cdot (r+1)^{4r^2+10r}. \tag{24}$$

On combining the estimate (15′) with David's Theorem 2.1 and observing the relations (20) - (24), 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*

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

satisfies the estimates

$$\begin{aligned} &\exp\Big\{ - Ch^{r+1}\big(\log(\tfrac{r+1}{2}gN) + 1\big)\,\big(\log\log(\tfrac{r+1}{2}gN) + 1\big)^{r+1} \prod_{i=1}^{r} \log V_i \Big\} \\ &\quad \le |gu| \\ &\quad < \exp\Big\{ - \lambda_1 N^2 + c_1' + \log g \Big\}, \end{aligned}$$

where $N = \max\limits_{1 \le i \le r} \{|n_i|\}$.

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

Corollary. *Under the hypothesis of the proposition,*

$$Ch^{r+1}(\log(\tfrac{r+1}{2}gN) + 1)\,(\log\log(\tfrac{r+1}{2}gN) + 1)^{r+1} \prod_{i=1}^{r} \log V_i + c_1' + \log g > \lambda_1 N^2. \tag{25}$$

4 A bound for integral points

Of course, the inequality (25) 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 (1) of integral points $P \in E(\mathbb{Q})$. For this purpose, we first prove another lemma.

Lemma 2 *Let ρ, σ and h be real numbers satisfying*

$$\rho \geq 1,\ h \geq 1 \quad \textit{and} \quad \sigma > \max\Big\{\Big(\frac{e^2}{h}\Big)^h,\ 1\Big\}.$$

Then the largest solution $x_0 \in \mathbb{R}$ of the equation

$$x = \rho + \sigma \log^h x$$

satisfies the inequality

$$x_0 < 2^{2h}\rho\sigma \log^h(h^h\sigma).$$

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

$$N > \max\{e^e, (6r+6)^2\}, \tag{26}$$

we have in (25) the inequality

$$\begin{aligned} \big(\log(\tfrac{r+1}{2}gN) + 1\big)\big(\log\log(\tfrac{r+1}{2}gN) + 1\big)^{r+1} &< 2\log^{r+2} N \\ &= 2^{-(r+1)}\log^{r+2} N^2. \end{aligned} \tag{27}$$

Put

$$c_1 := \max\Big\{\frac{c_1' + \log g}{\lambda_1},\ 1\Big\} \quad \text{and} \quad c_2 := \max\Big\{\frac{C}{\lambda_1}, 10^9\Big\}\Big(\frac{h}{2}\Big)^{r+1}\prod_{i=1}^{r}\log V_i. \tag{28}$$

On replacing in (25) the middle term by the right hand side of (27), we derive from (25) the inequality

$$N^2 < c_1 + c_2 \log^{r+2} N^2. \tag{29}$$

Now we apply Lemma 2 to (29). Let $N_0 \in \mathbb{R}$ be the largest solution of the equation obtained by equating both sides of (29). Then the inequality (29) cannot hold for $N > N_0$. Taking

$$\rho := c_1,\ \sigma := c_2 \text{ and } h := r+2$$

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

$$N_0 < N_1 := \sqrt{c_1 c_2}\cdot 2^{r+2}\cdot \log^{\frac{r+2}{2}}(c_2\cdot(r+2)^{r+2}). \tag{30}$$

It is clear that the positive integers N satisfying (29) also satisfy (30) since, as we noted, (29) implies $N \leq N_0$. of course, by (22) and (25) we also have

$$N_1 > \max\{e^e, (6r+6)^2\},\ \sqrt{\frac{\log(2g) + c_1'}{\lambda_1}}. \tag{31}$$

On combining the relations (21), (24) and (30), we thus arrive at the following fundamental theorem.

Theorem. *Let*

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

be an integral point on the elliptic curve E over $\mathbb{Q}$, where $P_1, \ldots, P_r \in E(\mathbb{Q})$ 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

$$N \le \max\{N_1, \ \frac{V}{r}\} =: N_2,$$

where N_1 is defined by (30) *and V is given by*

$$V := \max_{1 \le i \le r} \{V_i\}$$

with the V_i's subject to (20).

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 and the real and complex period ω_1 and ω_2, respectively, so that the V_i can be determined in accordance with (20) and to show, how the bound in the Theorem can be used to compute all integral points in $E(\mathbb{Q})$.

5 Proofs

Proof of Lemma 1. We may assume without loss of generality that the largest real root $\alpha \in \mathbb{R}$ of the polynomial $p(x) = x^3 + ax + b$ in (8) is non-negative. For if α 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

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

Then the polynomial in $y := x + M$ with M as in (12)

$$q(y) := p(y - M)$$

has the largest root $\alpha + M \geq 0$. Put

$$\xi_0 := \left\{ \begin{array}{ll} 2\alpha + M & \text{if } \beta,\, \gamma \in \mathbb{R} \\ 2 \cdot \max\left\{\alpha,\, \dfrac{\beta+\gamma}{2}\right\} + M & \text{if } \beta,\, \gamma \in \mathbb{C}\backslash\mathbb{R} \end{array} \right\}$$

and choose $\xi \in \mathbb{R}$ according to

$$\xi > \max\{\xi_0,\, 0\}. \tag{32}$$

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

$$\beta_1 := \alpha - \beta > 0,\ \gamma_1 := \alpha - \gamma > 0.$$

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 $\beta + \gamma = \beta + \overline{\beta} < 2\alpha$. Then we have $\beta_1 > 0,\ \gamma_1 > 0$ under the first condition and $\beta_1 + \overline{\beta}_1 = 2\alpha - \beta - \overline{\beta} > 0$ under the second. Under both conditions we gather that, for $z > 0 \iff y > \alpha + M \iff x > \alpha$,

   $$r(z) > z^3$$

   and hence conclude that

   $$\int_{\xi-\alpha}^{\infty} \frac{dz}{\sqrt{r(z)}} < \int_{\xi-\alpha}^{\infty} \frac{dz}{z^{\frac{3}{2}}} = \frac{2}{\sqrt{\xi - \alpha}}. \tag{33}$$

Now if $\beta,\ \gamma \in \mathbb{R}$, we conclude from

$$\tfrac{1}{2}\xi > \alpha + \tfrac{M}{2}$$

by (12) and (32) that

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

since $M \geq 0$, 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 $\xi > 2\alpha + M$ by (12) and (32).

2. Suppose now that $\beta, \gamma \in \mathbb{C}\backslash\mathbb{R}$ but $\beta + \gamma = \beta + \overline{\beta} \geq 2\alpha$. Then we have

$$\beta_1 + \overline{\beta}_1 = 2\alpha - \beta - \overline{\beta} \leq 0,$$

hence

$$z \geq z + \frac{\beta_1 + \overline{\beta}_1}{2}$$

and furthermore,

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

Altogether, for $z > 0 \iff x > \alpha$, this leads to the inequality

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

The integral (33) can therefore be estimated as follows:

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

But in this case, since by (12) and (32)

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

we infer

$$\frac{2}{\sqrt{\xi-\alpha+\frac{\beta_1+\overline{\beta}_1}{2}}} < \frac{\sqrt{8}}{\sqrt{\xi+M}} \leq \frac{\sqrt{8}}{\sqrt{\xi}}$$

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

Proof of Lemma 2. By Lemma 2.2 of [PdW], the largest solution $x_0 \in \mathbb{R}$ of the equation

$$x = A + B \cdot \log^h x$$

satisfies

$$x_0 < 2^h \left(A^{\frac{1}{h}} + B^{\frac{1}{h}} \log(h^h B) \right)^h.$$

Since A and B are at least 1, we have

$$A^{\frac{1}{h}} + B^{\frac{1}{h}} \log(h^h B) \leq 2A^{\frac{1}{h}} B^{\frac{1}{h}} \log(h^h B),$$

and this implies the asserted inequality

$$x_0 < 2^{2h} AB \log^h(h^h B),$$

thus proving Lemma 2.

In the above Proposition, we need to determine the numbers $V_i \in \mathbb{R}$ in accordance with the estimates (20). 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 ω_1 and ω_2, respectively, giving $\tau = \frac{\omega_2}{\omega_1}$. To calculate ω_1 and ω_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 arithogeometric mean of Gauss as described by Grayson [Gr]. For the computation of the elliptic logarithms u_i of the points P_i $(1 \leq i \leq r + 1)$ we use the fast-converging series given by Zagier [Za], formula (10). Of course, the Néron-Tate height of the basis points $P_1, \ldots, P_r$ of $E(\mathbb{Q})$, also required in (20), is calculated by the well-known procedure already employed in [GZ].

6 Reduction of the initial bound

The upper bound for N obtained in the Theorem in general is 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 turns out to be possible to eventually solve the elliptic equation in rational integers. The inequality

$$\left| n_0' + \sum_{i=1}^{r} n_i' u_i \right| < \exp\{-\lambda_1 N^2 + c_1' + \log g\} \tag{34}$$

obtained in the Proposition for $u' = gu$ in accordance with (16′), together with the inequallity $N \leq N_2$ established in the Theorem may be considered as a homogeneous diophantine approximation problem. Analogous inequaltities 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 adequate 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 Γ be the lattice spanned by the rows of the matrix

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

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

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

then (34) has no solution satisfying

$$\sqrt{\frac{1}{\lambda_1} \log \frac{C_0(c_1' + \log g)}{\tilde{N}}} \leq N \leq \tilde{N}. \tag{35}$$

To find an $\tilde{N}$ enjoying these properties, one chooses C_0 in the order the magnitude of N_1^{r+1} and computes the LLL-reduced basis [LLL] $b_1, \dots b_{r+1}$ of Γ. By proposition (1.11) of [LLL], we have

$$l(\Gamma) \geq 2^{-\frac{r}{2}} \|b_1\|,$$

where $\|b_1\|$ is the Euclidean length of the vector b_1. Now we take

$$\tilde{N} := \|b_1\| \cdot 2^{-\frac{r}{2}} \sqrt{r^2+5r+4}.$$

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

$$N \leq \sqrt{\frac{1}{\lambda_1} \log \frac{C_0(c_1' + \log g)}{\tilde{N}}}.$$

This process is iterated until the upper bound cannot be reduced further. Let N_1' be the result of the last iteration. In the range we are left left with after the reductions, i.e. for the vectors

$$(n_0, \dots, n_r) \in \mathbb{Z}^{r+1}$$

such that

$$\max_{1\le i\le r}\{|n_i|\} \le N_1',$$

we now test all points

$$n_1P_1 + \ldots + n_rP_r + P_{r+1}$$

in (1) for integrality.

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

7 Examples

We take the elliptic curve from Mestre [Me]

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

and consider the quasiminimal model in short Weierstrass form

$$y^2 = x^3 - 1642032x + 628747920$$

with discriminant

$$\Delta = 112571102923779428352 = 2^12 * 3^12 * 51714450757,$$

modular invariant

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

and height of E

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

E has rank

$$r = 6$$

and torsion group

$$E_{\mathrm{tors}}(\mathbb{Q}) = \{\mathcal{O}\},$$

[1] After we had finished writing this paper, we learned about a lecture of Tzanakis delivered in October 1993 at Oberwolfach in which he also reported on an algorithm for computing integral points on elliptic curves by means of elliptic logarithms.

The following six points form a basis of the Mordell-Weil group $E(\mathbb{Q})$, where we exhibit also their canonical height $\hat{h}$

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

The symmetric matrix of the bilinear from associated with the quadratic form $\hat{h}$ 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

$$\begin{aligned} \chi_A(x) &= x^6 - 20.85013503\,x^5 + 164.9142957\,x^4 - 618.6663540\,x^3 \\ &\quad +1125.293711\,x^2 - 906.8522386\,x + 226.2807738. \end{aligned}$$

The eigenvalues of A are

$$\lambda_1 = 0.4323724011$$
$$\lambda_2 = 1.5647578466$$
$$\lambda_3 = 1.9944764779$$
$$\lambda_4 = 4.3502898759$$
$$\lambda_5 = 5.5014070699$$
$$\lambda_6 = 7.0068311531$$

of which λ_1 is needed in (4).

The real period appearing in (10) is

$$\omega_1 = 1.0582679843$$

and the complex period

$$\omega_2 = 0.4067231150\, i$$

giving

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

Hence the constant in (16) becomes

$$c_1' = 1.4451852966$$

thus yielding the constant in (28)

$$c_1 = \max\left\{\frac{c_1' + \log 1}{\lambda_1},\ 1\right\} = 1.4451852966$$

In (14) we need the elliptic logarithms of the basis points $P_1, \ldots, P_6$:

$$u_1 = 0.0011316844$$
$$u_2 = 0.0649588423$$
$$u_3 = 0.0912606341$$
$$u_4 = 0.4447562185$$
$$u_5 = 0.1867017663$$
$$u_6 = 0.2047900792$$

and the quantity

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

whence

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

Therefore we may choose

$$V_i = e^h = 130061413389624701760 \qquad (i = 1, \ldots, 6)$$

in accordance with (20). It turns out that (21) is automatically satisfied if we take

$$B = 6N$$

according to (23). The constant C in (24) is

$$C \sim 7 * 10^{213}$$

and therefore, the constant c_2 in (29) becomes

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

Finally in (30) we get

$$N_1 = 1.1 * 10^{126}$$

and the Theorem shows that

$$N \leq \max\left\{N_1, \frac{e^h}{6}\right\} = N_1.$$

Now we apply de Weger reduction to the $(r+1) \times (r+1)$ matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ C_0 \cdot u_1 & C_0 \cdot u_2 & C_0 \cdot u_3 & C_0 \cdot u_4 & C_0 \cdot u_5 & C_0 \cdot u_6 & C_0 \end{pmatrix}$$

starting with the value

$$C_0 = 10^{890}.$$

After the first reduction, the length of the shortest vector b_1 of the lattice is at least

$$\|b_1\| \geq 3.6 * 10^{-653}$$

and we obtain the new upper bound

$$N \leq 59.$$

A second application of de Weger reduction with the startng value

$$C_0 = 10^{17}$$

reduces the length of the shortest vector b_1 of the lattice to at least

$$\|b_1\| \geq 1.7 * 10^{-16}$$

and yields

$$N \leq 9.$$

The third de Weger reduction with the starting value

$$C_0 = 10^{14}$$

yields the length of b_1 at least

$$\|b_1\| \geq 7.5 * 10^{-14}$$

and improves the upper bound to

$$N \leq 8.$$

A fourth reduction leads to the same upper bound for N so that we stop here.

It remains therefore to test all the points

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

with respect to integrality.

In addition we have to test all points $P = (\xi, \eta) \in E(\mathbb{Q})$ such that

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

in order to take care of the case in which $(7')$ rather than (7) is valid. In this extra search procedure we did not find any new points.

Altogether we obtain the following 70 integral points (and their additive inverses, of course) on E over $\mathbb{Q}$:

Table

No.	P	n_1	n_2	n_3	n_4	n_5	n_6	$\hat{h}(P)$
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

Table (suite)

No.	P	n_1	n_2	n_3	n_4	n_5	n_6	$\hat{h}(P)$
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 (suite)

No.	P	n_1	n_2	n_3	n_4	n_5	n_6	$\hat{h}(P)$
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

Table (suite)

No.	P	n_1	n_2	n_3	n_4	n_5	n_6	$\hat{h}(P)$
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

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. Proc. Ramanujan Centennial Intern. Conf., Annamalainagar, December 1987, 31-43.

[GPP] I. Gaàl, A. Pethö and M. Pohst, On the Resolution of Index Form Equations in Biquadratic Number Fields II. J. Numb. Th. **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.

[GZ] J. Gebel and H. G. Zimmer, Computing the Mordell-Weil Group of an Elliptic Curve over $\mathbb{Q}$. To appear in CRM Proceedings.

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

[Gr] D. R. Grayson, The arithogeometric Mean. Arch. Math. **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] S. Lang, Elliptic Functions. Addison Wesley Publ. Co., Reading 1973.

[L3] S. Lang, Elliptic Curves: Diophantine Analysis. Grundl. d. math. Wiss. **231**, Springer Verlag, Berlin 1978.

[L4] S. Lang, Conjectured Diophantine Estimates on Elliptic Curves. Progr. in Math. **35**, 155-171. Birkhäuser Verlag, Basel 1983.

[LLL] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring Polynomials with Rational Coefficients, Math. Ann. **261** (1982), 515-534.

[M] Y. I. Manin, Cyclotomic Fields and Modular Curves. Russian Math. Surveys **26** (1971), no. 6, 7-78.

[Mz] B. Mazur, Rational Points on Modular Curves, Modular Functions of One Variable V, Lect. Notes in Math. **601** (1977), 107-148, Springer-Verlag.

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

[PS] A. Pethö and R. Schulenberg, Effektives Lösen von Thue Gleichungen. Publ. Math. Debrecen **34** (1987), 189-196.

[PdW] A. Pethö 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.

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

[Sch, Th. 2] W. Schmidt, Integer Points on Curves of Genus 1. Compos. Math. **81** (1992), 33-59.

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

[Si2] J. H. Silverman, 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.

[TdW] N. Tzanakis and B. M. M. de Weger, On the Practical Solution of the Thue Equation. J. Numb. Th. **31** (1989), 99-132.

[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. Numb. Th. **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] H. G. Zimmer, On Manin's conditional Algorithm. Bull. Soc. Math. France, Mémoire N^o **49-50** (1977), 211-224.

[Zi3] H. G. Zimmer, Generalization of Manin's Conditional Algorithm. SYMSAC 76. Proc. ACM Sympos. Symbolic Alg. Comp. Yorktown Heights, N.Y., 1976, 285-299.

[Zi4] H. G. Zimmer, Computational Aspects of the Theory of Elliptic Curves. Numb. Th. and Appl., Ed. R. A. Mollin, Kluwer Acad. Publ. 1989, 279-324.

[Zi5] H. G. Zimmer, A Limit Fromula for the Canonical Height of an Elliptic Curve and its Application to Height Computations. Number Theory. Ed. R. A. Mollin, W. de Gruyter Verlag, Berlin and New York 1990, 641-659.