

Solving Elliptic Diophantine Equations by Estimating Linear Forms in Elliptic Logarithms

R.J. Stroeker* and N. Tzanakis†

Abstract

In order to compute all integer points on a Weierstraß equation for an elliptic curve E/\mathbb{Q} , one may translate the linear relation between rational points on E into a linear form of elliptic logarithms. An upper bound for this linear form can be obtained by employing the Néron-Tate height function and a lower bound is provided by a recent theorem of S. David. Combining these two bounds allows for the estimation of the integral coefficients in the group relation, once the group structure of $E(\mathbb{Q})$ is fully known. Reducing the large bound for the coefficients so obtained to a manageable size is achieved by applying a reduction process due to de Weger. In the final section two examples of elliptic curves of rank 2 and 3 are worked out in detail.

1 Introduction

In [Z], Zagier describes several methods for explicitly computing (large) integral points on models of elliptic curves defined over \mathbb{Q} . Here we are interested in the computation of all integral points on a given Weierstraß equation for an elliptic curve E/\mathbb{Q} , but not merely by reducing the original diophantine equation to an equivalent finite set of Thue equations which are subsequently solved by elementary, algebraic or analytic methods (see [TdW] and [STz]). On the contrary, we adopt a more natural approach, one in which the linear (group) relation between an integral point and the generators of the free component of the Mordell-Weil group is directly transformed into a linear form in elliptic logarithms. This idea is not new; see [Ma, App. IV], [La, Ch. VI, § 8], and [S1, Ch. IX, § 5]. To make it

*Econometric Institute, Erasmus University Rotterdam, P.O. Box 1738, 3000 DR Rotterdam, The Netherlands; e-mail: stroeker@wis.few.eur.nl

†Department of Mathematics, University of Crete, P.O. Box 470, 714 09 Iraklion, Greece; e-mail: tzanakis@grearn.bitnet

work, that is to say, in order to produce upper bounds for the coefficients in the original linear (group) relation, one needs an effective lower bound for the linear form in elliptic logarithms. First to obtain such lower bounds were D.W. Masser [Ma, App. IV], in the case of elliptic curves with complex multiplication, and G. Wüstholz [Wu]; see also the bibliography in [H]. We felt that the recent result of N. Hirata-Kohno [H, Coroll. 2.16] should serve our purpose best. Unfortunately, this result, being rather more general than we required, though effective, is not completely explicit. At our request, S. David kindly undertook the highly non-trivial task of making explicit the special case we needed. It is S. David's result [D, Th. 2.1] that is applied here for the first time to provide explicit upper bounds for the coefficients in the linear (group) relation corresponding to a given Weierstraß equation. We shall show by example that these bounds may be reduced to manageable proportions.

In the following sections we shall give a detailed description of the method referred to above. In the final section we present two examples, worked out in detail, of elliptic curves taken from the literature. Our choice seems rather arbitrary, but both examples are of some interest as illustrations of the method, and also in view of the difficulties one has to overcome when trying to solve the corresponding diophantine equations by traditional methods.

The equations referred to above are

$$6y^2 = (x + 1)(x^2 - x + 6),$$

and

$$y^2 = (x + 337)(x^2 + 337^2).$$

The corresponding elliptic curves have rank 2 and 3 respectively.

2 Preliminaries

This section is devoted to the introduction of the necessary concepts and to setting up the relevant notation.

We are interested in computing explicitly all solutions $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ of the equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad (1)$$

where a_1, a_2, a_3, a_4, a_6 are rational integers. This equation defines an elliptic curve E/\mathbb{Q} , provided it has a non-vanishing discriminant. From now on we assume that this is the case.

A linear transformation

$$X = u^2x + v, \quad Y = u^3y + wu^2x + z \quad (2)$$

for suitably chosen $u, v, w, z \in \mathbb{Q}$, $u \neq 0$, gives another equation for E of the form

$$y^2 = f(x), \quad (3)$$

where $f \in \mathbb{Q}[x]$ is a cubic polynomial

$$f(x) = x^3 + ax + b$$

with non-zero discriminant. The latter equation (3) is often more convenient. Throughout this paper, an *integral point* will always be a point $P = (X(P), Y(P))$ with rational integral coordinates satisfying (1); the possibly non-integral coordinates of the point P on the corresponding equation (3), will be denoted by $(x(P), y(P))$.

Let r be the rank of the Mordell-Weil group $E(\mathbb{Q})$. We assume $r \geq 1$ as the case $r = 0$ is rather trivial. By the Mordell-Weil theorem we have the following group isomorphism

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

The set of generators of $E(\mathbb{Q})/E_{tors}(\mathbb{Q})$ will be denoted by $\{P_1, \dots, P_r\}$. We shall always tacitly assume that such a set can be explicitly determined.

For any $P \in E(\mathbb{Q})$, there exist rational integers m_1, \dots, m_r such that

$$P = m_1 P_1 + \dots + m_r P_r + T \quad (4)$$

for some $T \in E_{tors}(\mathbb{Q})$. The construction of the (finite) torsion group $E_{tors}(\mathbb{Q})$ should not pose any problems, so that (4) can be seen as a direct link between the (unknown) point P and the integral vector $\mathbf{m} = (m_1, \dots, m_r)$. For integral P we would like to estimate the vector \mathbf{m} . This should be possible, at least in principle, as the number of such points P is finite. In other words, if the integral point $P = (X(P), Y(P))$ satisfies (1), then $|X(P)|$ and $|Y(P)|$ are bounded, which means that P cannot be too close to the identity O of the group $E(\mathbb{Q})$.

In order to use the information provided by (4) numerically, we need a real valued function that does not disturb the linear character of (4), that maps the identity O to 0 and measures in some sense the distance from O . Now, the group $E(\mathbb{R})$ is isomorphic to one or two copies of the circle group \mathbb{R}/\mathbb{Z} , depending on the number of real zeros of $f(x)$. Let γ be the largest (possibly the only) real root of $f(x) = 0$. As the integral points P satisfying $X(P) < u^2\gamma + v$ can be easily found by direct search, we'll concentrate on those integral P which belong to the component of $E(\mathbb{R})$ containing the identity O (i.e. the infinite component), namely

$$E_0(\mathbb{R}) = \{P \in E \cap \mathbb{R}^2 \mid x(P) \geq \gamma\} \cup \{O\}.$$

The group isomorphism

$$\phi : E_0(\mathbb{R}) \longrightarrow \mathbb{R}/\mathbb{Z}$$

can be given explicitly as follows.

Let $\omega = 2 \int_{\gamma}^{\infty} \frac{dt}{\sqrt{f(t)}}$. This is the fundamental real period of the Weierstraß \wp -function associated with the curve given by (3). For $P \in E_0(\mathbb{R})$ (see [Z, p. 429]),

$$\phi(P) \equiv \begin{cases} 0 \pmod{1} & \text{if } P = O, \\ \frac{1}{\omega} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{f(t)}} \pmod{1} & \text{if } y(P) \geq 0, \\ -\phi(-P) \pmod{1} & \text{if } y(P) \leq 0. \end{cases} \quad (5)$$

Clearly, there is no loss of generality in assuming that $\phi(P) \in [0, 1)$.

It is our goal to establish an effectively computable upper bound for $|\phi(P)|$ depending on the coefficients m_1, \dots, m_r only. Because of (4) this results in an upper bound for a linear form in $\phi(P_1), \dots, \phi(P_r)$, essentially the elliptic logarithms. Combining this upper bound with David's lower bound for linear forms in elliptic logarithms (see [D, Th. 2.1] and the Appendix) clinches the argument in so far as an effectively computable upper bound for $\max_{1 \leq i \leq r} |m_i|$ is obtained in this way.

In the course of finding the upper bound for $|\phi(P)|$ we mentioned above, we need the *canonical* or *Néron-Tate height* function \hat{h} . This function is a positive definite quadratic form on $E(\mathbb{Q})/E_{tors}(\mathbb{Q})$. To be more precise—we follow Silverman, see [S1, Ch. VIII, §9)—if

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

is the so-called *Néron-Tate* (or *Weil*) *pairing*, and P is expressed as in (4), then

$$\hat{h}(P) = \frac{1}{2} \sum_{1 \leq i, j \leq r} \langle P_i, P_j \rangle m_i m_j \quad (6)$$

and the matrix $\mathcal{H} = (\frac{1}{2} \langle P_i, P_j \rangle)_{r \times r}$ is positive definite (see [S1, Prop. 9.6, p. 232]). Relation (6) immediately follows from the facts that for any $P \in E(\overline{\mathbb{Q}})$ and any $m \in \mathbb{Z}$

- the Néron-Tate pairing is bilinear,
- $\hat{h}(mP) = m^2 \hat{h}(P)$,
- $\hat{h}(P) \geq 0$ and $\hat{h}(P) = 0$ if and only if P is a torsion point.

3 Basic inequalities

In this section we shall establish a few elementary inequalities that are crucial in the derivation of our upper bound for $|\phi(P)|$. In each inequality we introduce an absolute constant accordingly labeled.

Inequality 1. *Let $P \in E(\mathbb{Q})$ be expressed as in (4). Then*

$$\hat{h}(P) \geq c_1 \max_{1 \leq i \leq r} m_i^2,$$

where c_1 is the least eigenvalue of the positive definite matrix \mathcal{H} introduced in (6).

Proof. According to (6) we have

$$\hat{h}(P) = \mathbf{m}^T \mathcal{H} \mathbf{m},$$

where \mathbf{m} is the column vector with components m_1, \dots, m_r . As \mathcal{H} is symmetric, a diagonal matrix Λ of eigenvalues of \mathcal{H} and an orthogonal matrix \mathcal{Q} exist such that $\mathcal{H} = \mathcal{Q}^T \Lambda \mathcal{Q}$. Writing $\mathbf{n} = \mathcal{Q} \mathbf{m}$ and observing that $\mathcal{Q}^T \mathcal{Q} = I$, we deduce

$$\begin{aligned} \hat{h}(P) &= \mathbf{m}^T \mathcal{Q}^T \Lambda \mathcal{Q} \mathbf{m} = \mathbf{n}^T \Lambda \mathbf{n} = \sum_{i=1}^r \lambda_i n_i^2 \\ &\geq c_1 \sum_{i=1}^r n_i^2 = c_1 \mathbf{n}^T \mathbf{n} = c_1 \mathbf{m}^T \mathcal{Q}^T \mathcal{Q} \mathbf{m} = c_1 \mathbf{m}^T \mathbf{m} \\ &= c_1 \sum_{i=1}^r m_i^2 \geq c_1 \max_{1 \leq i \leq r} m_i^2, \end{aligned}$$

as claimed. □

Inequality 2. *Let $\gamma, \gamma', \gamma''$ be the roots of $f(x) = 0$ and put $c_2 = 2 \max\{|\gamma|, |\gamma'|, |\gamma''|\}$. Then, for all $x \geq c_2$,*

$$\left| \int_x^\infty \frac{dt}{\sqrt{f(t)}} \right| \leq 4\sqrt{2}|x|^{-1/2}.$$

Proof. For $t \geq x \geq c_2$ we have $0 < f(t) = t^3 + at + b = |t - \gamma| |t - \gamma'| |t - \gamma''|$ and as t is larger than the absolute largest zero of $f(x)$, it follows that $|t - \gamma| \geq t - |\gamma| \geq t/2$, and likewise for γ' and γ'' . Consequently, $1/\sqrt{f(t)} \leq 2^{3/2} t^{-3/2}$ and hence, for all $N > x$,

$$\int_x^N \frac{dt}{\sqrt{f(t)}} \leq \int_x^N 2^{3/2} t^{-3/2} dt = 4\sqrt{2}(x^{-1/2} - N^{-1/2}).$$

Letting N tend to infinity completes the proof. □

Before proceeding, let us remind the reader that there is another, in some sense more natural height function than the canonical height \hat{h} . For any rational number $\rho = m/n$ with $\gcd(m, n) = 1$,

$$h(\rho) := \log \max\{|m|, |n|\}$$

is known as the *absolute logarithmic height* of ρ . Now the *naive height* of a point $P \in E(\mathbb{Q})$, $P \neq O$, is defined as the absolute logarithmic height of $X(P)$.

Inequality 3. *Let u, v and γ be as in Section 2. Let X_0 be a positive integer strictly larger than v . Put*

$$c_0 = \begin{cases} \log |u| & \text{if } v \leq 0, \\ \log |u| + \frac{1}{2}v(X_0 - v)^{-1} & \text{if } v > 0, \end{cases}$$

$$c_3 = c_0 + \frac{1}{12} \log |\Delta| + \frac{1}{12} \log^+ |j| + \frac{1}{2} \log^+ |b_2/12| + \frac{1}{2} \log 2^* + 1.07,$$

where Δ and j are the discriminant and the j -invariant of the elliptic curve E/\mathbb{Q} defined by (1), $\log^+ |\alpha| := \log \max\{1, |\alpha|\}$ for $\alpha \in \mathbb{R}$, $b_2 = a_1^2 + 4a_2$ and $2^* = 1$ or 2 according as b_2 vanishes or not, respectively.

Then, for all $P \in E(\mathbb{Q})$ with $X(P) \geq X_0$, we have $x(P) > 0$, and

$$\hat{h}(P) - \frac{1}{2} \log x(P) \leq c_3.$$

Remark. There is no restriction on the choice of model to which we apply Silverman's theorem [S3, Th. 1.1], so long as $a_1, \dots, a_6 \in \mathbb{Z}$. Therefore, we may choose a model that provides a small constant c_3 , subject to $a_1, \dots, a_6 \in \mathbb{Z}$. A natural choice is the global minimal Weierstraß model, or the model that minimizes $\log^+ |b_2/12|$.

Proof. Clearly $x(P) = u^{-2}(X(P) - v) > 0$. Next, by [S3, Th. 1.1] we have

$$\hat{h}(P) - \frac{1}{2}h(X(P)) \leq c_3 - c_0 \quad (7)$$

and, since P is an integral point, $h(X(P)) = \log X(P)$. Therefore

$$h(X(P)) = \log(u^2x(P) + v) = 2 \log |u| + \log x(P) + \log \left(1 + \frac{v}{u^2x(P)}\right). \quad (8)$$

If $v \leq 0$ then the final logarithm in (8) is non-positive, and for positive v

$$\log \left(1 + \frac{v}{u^2x(P)}\right) < \frac{v}{u^2x(P)} = \frac{v}{X(P) - v} \leq \frac{v}{X_0 - v}.$$

Combining this with (7) and (8) completes the proof. \square

4 The linear form in elliptic logarithms

As we are interested in finding all integral points on (1), and as points with small X -coordinate can be found without fail by direct search, we focus our attention on points $P \in E_0(\mathbb{Q})$, $P \neq O$ with $X(P) \geq X_0$, for some conveniently chosen positive integer X_0 . Elaborating on this choice of X_0 , we first point out that a point P of $E(\mathbb{R})$ belongs to $E_0(\mathbb{R})$ if and only if $x(P) \geq \gamma$ or, equivalently, if and only if $X(P) \geq u^2\gamma + v$. In view of this and the requirements set down in Inequalities 2 and 3, we take $X_0 = \lfloor \max\{c_2, u^2\gamma + v, v\} \rfloor + 1$.

Let P be expressed in terms of the generators of the free component of $E(\mathbb{Q})$ as in (4). We put

$$M = \max_{1 \leq i \leq r} |m_i|.$$

Applying the isomorphism ϕ to (4) yields

$$\phi(P) \equiv m_1\phi(P_1) + \cdots + m_r\phi(P_r) + \phi(T) \pmod{1},$$

and hence an integer m_0 exists such that

$$\phi(P) = m_0 + m_1\phi(P_1) + \cdots + m_r\phi(P_r) + \phi(T), \quad (9)$$

so that, assuming all ϕ -values belong to $[0, 1)$,

$$|m_0| < |m_1| + \cdots + |m_r| + 1 \leq rM + 1. \quad (10)$$

For our purpose, it clearly suffices to compute an upper bound for M .

Let t be the order of the torsion point T . Then, $t\phi(T) \equiv \phi(O) \equiv 0 \pmod{1}$, and hence $\phi(T) = s/t$, for some non-negative integer $s < t$. Thus,

$$\phi(P) = (m_0 + \frac{s}{t}) + m_1\phi(P_1) + \cdots + m_r\phi(P_r). \quad (11)$$

On the other hand, by Inequalities 1 and 3,

$$\log x(P) \geq 2(\hat{h}(P) - c_3) > 2(c_1M^2 - c_3).$$

Therefore, $|x(P)|^{-1/2} = (x(P))^{-1/2} \leq \exp(c_3 - c_1M^2)$. In view of Inequality 2 and the definition of ϕ , it follows that

$$|\phi(P)| = \left| \frac{1}{\omega} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{f(t)}} \right| \leq \frac{4\sqrt{2}}{\omega} |x(P)|^{-1/2} \leq \frac{4\sqrt{2}}{\omega} \exp(c_3 - c_1M^2). \quad (12)$$

On writing

$$L(P) := \omega\phi(P) = (m_0 + \frac{s}{t})\omega + m_1u_1 + \cdots + m_ru_r, \quad (13)$$

where $u_i = \omega\phi(P_i)$ for $i = 1, \dots, r$, we see that (12) induces the upper bound for the linear form $L(P)$ in elliptic logarithms hinted at above. Indeed, if we denote by \wp the Weierstraß \wp -function, which parameterizes E , then

$$\wp(u_i) = \wp\left(\int_{x(P)}^{\infty} \frac{dt}{\sqrt{f(t)}}\right) = x(P), \quad i = 1, \dots, r$$

(see for instance [WW, Ch. XX, no 20·221]). Note that ω is a pole of \wp . As the linear form $L(P)$ is non-vanishing, because $P \neq O$ implies $\phi(P) \neq 0$, we may apply S. David's theorem (see the Appendix) to obtain the lower bound

$$|L(P)| > \exp\left(-c_4(\log M' + c_5)(\log \log M' + c_6)^{r+2}\right) \quad (14)$$

for explicitly computable positive constants c_4 , c_5 and c_6 , where

$$\log M' := \max\{\log M, h(m_0 + s/t)\},$$

provided that M is not less than some explicitly computable constant $M_0 \geq 16$. Combining upper and lower bounds (12) and (14) then yields

$$c_1 M^2 < c_4(\log M' + c_5)(\log \log M' + c_6)^{r+2} + c_3 + \log(4\sqrt{2}). \quad (15)$$

By (10) and the definition of M' , we have

$$M' \leq |m_0 t + s| < t_0(rM + 1) + t_0 - 1, \quad t_0 := \max\{\text{order}(T) \mid T \in E_{\text{tors}}(\mathbb{Q})\},$$

where $t_0 \leq 12$ by Mazur's theorem (see [S1, p. 223]). From this inequality we easily deduce that

$$\log M' < \log M + \log(t_0 r) + \frac{2t_0 - 1}{16t_0 r},$$

so that (15) implies

Principal Inequality .

$$M^2 < c_3 c_1^{-1} + c_1^{-1} \log(4\sqrt{2}) + c_4 c_1^{-1} (\log M + c_7)(\log \log M + c_8)^{r+2}, \quad (16)$$

where

$$c_7 = c_5 + \log(t_0 r) + \frac{2t_0 - 1}{16t_0 r} \quad \text{and} \quad c_8 = c_6 + \left(\log(t_0 r) + \frac{2t_0 - 1}{16t_0 r}\right) / \log 16.$$

Now clearly (16) provides an effectively computable upper bound for M .

5 Reduction of the upper bound

Inequalities (12) and (16) may be rewritten in simplified form as

$$|\phi(P)| < K_1 \exp(-K_2 M^2) \quad \text{and} \quad M < K_3, \quad (17)$$

where K_1, K_2, K_3 are explicitly known and K_3 is “very large”—in the two numerical examples of section 6 it is of magnitude 10^{38} and 10^{59} , respectively. Since such a large upper bound for M is way out of reach of any practical search method, we’ll try to reduce it.

Consider the $(r + 1)$ -dimensional lattice, generated by the columns of the matrix

$$\mathcal{A} = \begin{pmatrix} 1 & \dots & 0 & 0 \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ [K_0\phi(P_1)] & \dots & [K_0\phi(P_r)] & K_0 \end{pmatrix}. \quad (18)$$

Here K_0 is a conveniently chosen integer, larger than K_3^{r+1} —this choice of K_0 will be further discussed in the lines following the Proposition. Further, $[\cdot]$ means rounding towards 0, i.e. $[\alpha] = \lceil \alpha \rceil$ if $\alpha \leq 0$, and $[\alpha] = \lfloor \alpha \rfloor$ if $\alpha > 0$.

Let $(m_1, \dots, m_r, m_0) \in \mathbb{Z}^{r+1}$ satisfy $|m_i| < K_3$ for $i = 0, 1, \dots, r$, and consider the lattice point

$$\ell = \mathcal{A} \begin{pmatrix} tm_1 \\ \vdots \\ tm_r \\ tm_0 + s \end{pmatrix} = \begin{pmatrix} tm_1 \\ \vdots \\ tm_r \\ \lambda \end{pmatrix},$$

where

$$\lambda := tm_1[K_0\phi(P_1)] + \dots + tm_r[K_0\phi(P_r)] + (tm_0 + s)K_0.$$

Since $|\lambda - K_0 t \phi(P)| \leq rtM \leq rtK_3$ —recall (11)—it follows that

$$\|\ell\|^2 = t^2(m_1^2 + \dots + m_r^2) + \lambda^2 \leq rt^2K_3^2 + t^2(K_0|\phi(P)| + rK_3)^2. \quad (19)$$

On the other hand, if the lattice basis $\{\mathbf{b}_1, \dots, \mathbf{b}_{r+1}\}$ is reduced in the sense of [LLL], we have

$$\|\mathbf{b}_1\|^2 \leq 2^r \|\ell\|^2,$$

in view of Proposition (1.11) of the paper cited. Combining this with (19) yields

$$K_0|\phi(P)| \geq \sqrt{t^{-2}2^{-r}\|\mathbf{b}_1\|^2 - rK_3^2} - rK_3, \quad (20)$$

which gives, after applying the first inequality of (17),

$$M^2 \leq K_2^{-1} \left(\log(K_0K_1) - \log(\sqrt{t^{-2}2^{-r}\|\mathbf{b}_1\|^2 - rK_3^2} - rK_3) \right), \quad (21)$$

provided the right-hand-side of (20) is positive, i.e.

$$\|\mathbf{b}_1\| > 2^{r/2}tK_3\sqrt{r^2 + r}. \quad (22)$$

We have thus proven the following

Proposition . *If the first vector \mathbf{b}_1 of an LLL-reduced basis for the lattice generated by the column vectors of the matrix A in (18) satisfies (22), then an upper bound for M is given by (21).*

Heuristically, it can be argued (see for instance [TdW, sect. 3.1]) that the length of \mathbf{b}_1 is of the same magnitude as $K_0^{1/(r+1)}$. Therefore, if we choose K_0 to be somewhat larger than $(2^{r/2}tK_3\sqrt{r^2 + r})^{r+1}$, it is reasonable to expect that (22) is satisfied—if not, we choose a larger K_0 —so that the Proposition can be applied. Note that the initial bound K_3 of M is thus reduced to a new bound which is of the size of $\sqrt{\log K_3}$. If the reduced bound is not small enough, then we repeat the above procedure with the reduced bound replacing K_3 .

For the computation of an LLL-reduced basis we have applied de Weger's version of the LLL-algorithm. For a detailed description the reader should consult de Weger's book [dW, Ch. 3].

6 Applications

In this section we shall apply the method described above to the two equations mentioned in the introduction.

The first application is about the determination of all integer points on Mordell's diophantine equation

$$6Y^2 = (X + 1)(X^2 - X + 6). \quad (23)$$

In his book [Mo, p. 259] Mordell asks whether all integer solutions of this equation are given by $X = -1, 0, 2, 7, 15, 74$. W. Ljunggren answered Mordell's question in [Lj] by adding one more point. Subsequently, Andrew Bremner gave a simpler proof in [Br]. Both methods are ingenious but complicated and their applicability to the general case appears to be limited. With our method the solution process is rather straightforward. We shall confirm that

Example 1. *The only integer solutions (X, Y) with $Y \geq 0$ of (23) are*

$$(-1, 0), (0, 1), (2, 2), (7, 8), (15, 24), (74, 260), (767, 8672).$$

In order to live up to this claim we have to construct a set of generators of infinite order for $E(\mathbb{Q})$, and the relevant constants have to be calculated. First we transform (23) to Weierstraß form. This gives

$$y^2 = x^3 + 180x + 1296. \quad (24)$$

The rank of the corresponding curve is 2; in fact Ian Connell's **Apecs** 2.7 gives this (complete) set of independent points of infinite order on (24): $\{(-3, 27), (10, 64)\}$. Further, the torsion subgroup $E_{tors}(\mathbb{Q})$ is of order two and its generator is $T = (-6, 0)$. It is not hard to show that the points $P_1 = (-3, 27)$ and $P_2 = (10, 64)$ generate the Mordell-Weil group modulo torsion. For, the set \mathcal{S} of 8 points $O, T, P_1, P_1 + T, P_2, P_2 + T, P_1 - P_2, P_1 - P_2 + T$ represents $E(\mathbb{Q})/2E(\mathbb{Q})$. Indeed, it is easily checked—again, **Apecs** is useful here, or one may use reduction modulo a few small primes—that none of these points, with the obvious exception of O , can be written as twice a point of $E(\mathbb{Q})$. Now by [S3, Prop. 7.2] the set of points P with

$$\hat{h}(P) \leq \max\{\hat{h}(X) \mid X \in \mathcal{S}\} \leq 0.8787$$

generates $E(\mathbb{Q})/E_{tors}(\mathbb{Q})$.

In order to set up a search for these points, we compare the canonical height with the naive height. Applying [S3, Th. 1.1] here yields

$$\frac{1}{2}h(X(P)) \leq \hat{h}(P) + \frac{1}{8}h(j) + \frac{1}{12}h(\Delta) + 0.973,$$

and, as

$$j_E = \frac{13500}{23}, \quad \text{and} \quad \Delta = -2^{16} 3^6 23,$$

this amounts to searching for all points $X(P) = R/S^2$ with $\max\{|R|, S^2\} < 3705$. We used **Upecs**—the little brother of **Apecs**, written in the very fast **UBASIC** 8.21 by Y. Kida—to perform this search, and as it happened, all points uncovered were linear combinations of P_1 , P_2 , and T .

In accordance with the definitions and notations as laid down in the Appendix at the end of this paper, we have $a = 2^2 3^2 5$, $b = 2^4 3^4$, and hence

$$\max\{1, |a/4|_p, |b/16|_p\} = \begin{cases} 3^4 & \text{if } p = \infty, \\ 1 & \text{otherwise,} \end{cases}$$

so that $h(a/4, b/16) \approx 4.3944492$. Also $h(j_E) = \log(13500) \approx 9.5104450$, and therefore

$$h_E \approx 9.5104450.$$

Also $\gamma = -6$ and the formulas (32) give

$$\begin{aligned} \omega_1 &\approx 1.0606085 + 0.81447364i, & \omega_2 &= \overline{\omega_1}, \\ \tau &= \frac{\omega_1}{\omega_2} \approx 0.25808531 + 0.96612213i, \end{aligned}$$

and the fundamental real period for the Weierstraß \wp -function associated with (24) is

$$\omega = 2\Re\omega_1 \approx 2.1212170.$$

Here we consider the following linear form in elliptic logarithms (see (13)):

$$L(P) = (m_0 + \frac{s}{2})\omega + m_1u_1 + m_2u_2.$$

In the notation of David's Theorem (see the Appendix) we have $r = 2$, $R_i = P_i$ ($i = 1, 2$), and $R_0 = O$. Also $u_i = \omega\phi(P_i)$ ($i = 1, 2$), and $u_0 = \omega$. Zagier's algorithm for the evaluation of the ϕ -values [Z, (10) on p. 430] gives

$$\phi(P_1) \approx 0.40084555, \quad \phi(P_2) \approx 0.25694930,$$

and hence, by the definition of the u_i 's, it follows that

$$u_1 \approx 0.85028037, \quad u_2 \approx 0.54504522.$$

Using **Apecs**—the algorithm in [S2] could also be used—we computed

$$\hat{h}(P_1) \approx 0.87867020, \quad \hat{h}(P_2) \approx 0.70055495,$$

and of course, $\hat{h}(R_0) = 0$.

Then, by the definition of the A_i 's, we see that we can take

$$A_0 = 24.55, \quad A_1 = A_2 = 9.511, \quad \mathcal{E} = e.$$

It follows that we may choose in (16)

$$c_4 = 9.655 \times 10^{69}.$$

Further, with $t_0 = 2$, $c_5 = 1$, $c_6 = 1 + h_E$ in (16), we can also choose

$$c_7 = 2.434, \quad c_8 = 11.03.$$

In (2) we take

$$u = 1, \quad v = w = z = 0,$$

so that, in particular, $X(P) = x(P)$. Using **MapleV** and **Apecs** we computed the least eigenvalue of the matrix \mathcal{H} introduced in (6), and we found (see Inequality 1)

$$c_1 \approx 0.26833321.$$

We choose $c_1 = 0.2683$ in (16). Moreover, we have

$$\gamma = -6, \quad \gamma' = 3 + 3\sqrt{23}i, \quad \gamma'' = \overline{\gamma'}$$

which gives, by Inequality 2,

$$c_2 = 12\sqrt{6}.$$

In the first paragraph of section 4, it was observed that X_0 may be chosen as $\lfloor \max\{c_2, u^2\gamma + v, v\} \rfloor + 1 = 30$, so that our search concerns all points P with

$X(P) \geq 30$. It is straightforward to check, even by hand, that the only integral points (x, y) on (24) with $x < 30$ are

$$(-6, 0), (0, 36), (12, 72).$$

By Inequality 3, $c_3 \approx 3.3360395$, so we can take

$$c_3 = 3.337$$

and (16) now yields

$$M < 4.368 \times 10^{38}.$$

Next we apply the reduction process of section 5 to the relevant linear form $\phi(P)$ (see (11)). In view of (12) we may take

$$K_1 = 75.03 > \frac{4\sqrt{2}}{\omega} \exp(c_3), \quad K_2 = 0.2683$$

and, because of the upper bound for M ,

$$K_3 = 4.368 \times 10^{38}.$$

Further, we choose

$$K_0 = 10^{120},$$

which is somewhat larger than $(4\sqrt{6}K_3)^3$.

In view of (18), this choice of K_0 forces us to compute $\phi(P_i)$ for $i = 1, 2$ with a precision of 120 decimal digits. This is accomplished by executing Zagier's algorithm ([Z, (10) on p. 430] coded in **UBASIC**, which allows for very large precision. Finally, application of the LLL-algorithm—we used de Weger's version [dW, sect. 3.5] and checked the result with the *lllint* procedure which is part of **GP/PARI 1.37.3**—gives a reduced basis $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ with

$$\mathbf{b}_1 = (-6.476 \cdots \times 10^{39}, -4.976 \cdots \times 10^{39}, 3.834 \cdots \times 10^{39}),$$

from which we see that the inequality (22) with $r = t = 2$ is satisfied. Hence, by the Proposition of section 5, $M \leq 26$. Repeating the process with K_1, K_2 as above and $K_3 = 26, K_0 = 10^8$, the LLL-algorithm gives a reduced basis with

$$\mathbf{b}_1 = (-101, -146, 266).$$

Thus, (22) is satisfied and the Proposition yields the new bound

$$M \leq 8.$$

The result of a direct search—using **Apeps** again—for all integral points

$$P = m_1 P_1 + m_2 P_2 + \epsilon T, \quad 0 \leq m_1 \leq 8, \quad |m_2| \leq 8, \quad \epsilon \in \{0, 1\}$$

with $(x(P), y(P))$ on (24) and $x(P) \geq 30$ is listed in the following table:

m_1	m_2	ϵ	$x(P)$	$y(P)$
0	-2	1	4602	-312192
0	2	1	4602	312192
1	-2	0	69	-585
1	-1	0	42	288
1	0	1	90	-864
2	-1	1	444	9360

From this we see that the only integral solutions (x, y) of (24) are those given by the $x(P)$ -values in the table in addition to those given by $x = -6, 0, 12$. Since the solutions (X, Y) of (23) and (x, y) of (24) are related by

$$x = 6X, \quad y = 36Y,$$

and as all x -values mentioned above, except 69, are divisible by 6, the integer solutions of (24) are as claimed in Example 1.

The next example deals with the Weierstraß equation

$$Y^2 = (X + 337)(X^2 + 337^2). \quad (25)$$

We'll show that

Example 2. *The only integer solutions (X, Y) with $Y \geq 0$ of (25) are*

$$(-337, 0), (-287, 3130), (2113, 105910), (56784, 13571615).$$

Necessary information on the characteristics of the elliptic curve given by (25) can be found in [STo]. In particular, $E_{tors}(\mathbb{Q}) \cong \mathbb{Z}_2$ with point of order two $T := (-337, 0)$ and set of generators $\{P_1, P_2, P_3\}$ of $E(\mathbb{Q})/E_{tors}(\mathbb{Q})$, where

$$P_1 = \left(\frac{5392}{9}, \frac{567845}{27} \right), \quad P_2 = (56784, 13571615), \quad P_3 = \left(\frac{105144}{25}, \frac{35547097}{125} \right).$$

Further

$$a = \frac{2}{3} \cdot 337^2, \quad b = \frac{20}{27} \cdot 337^3, \quad j_E = 128, \quad \text{and} \quad \Delta = -2^8 337^6.$$

By (32) of the Appendix we computed the following pair of fundamental periods:

$$\omega_1 \approx 0.21988008 + 0.14965789i, \quad \omega_2 = \overline{\omega_1},$$

and thus

$$\tau = \frac{\omega_1}{\omega_2} \approx 0.36680841 + 0.93029651i,$$

which satisfy the requirements of (30). It follows that

$$\omega = 2\Re\omega_1 \approx 0.43976016$$

is a fundamental real period.

Next we computed $h(a/4, b/16)$. As

$$\max\{1, |a/4|_p, |b/16|_p\} = \begin{cases} 2^{-2} 3^{-3} 5 \cdot 337^3 & \text{if } p = \infty, \\ 2^2 & \text{if } p = 2, \\ 3^3 & \text{if } p = 3, \\ 1 & \text{otherwise,} \end{cases}$$

we see that

$$h_E = h\left(\frac{a}{4}, \frac{b}{16}\right) \approx 19.069687.$$

Here we consider the linear form in elliptic logarithms (see (13))

$$L(P) = (m_0 + \frac{s}{2})\omega + m_1u_1 + m_2u_2 + m_3u_3.$$

In the notation of David's Theorem (see the Appendix) we now have $r = 3$, $R_i = P_i$ ($i = 1, 2, 3$), and $R_0 = O$. Also, $u_i = \omega\phi(P_i)$ for $i = 1, 2, 3$, and $u_0 = \omega$. Zagier's algorithm for the evaluation of the ϕ -values [Z, (10) on p. 430]) gives

$$\phi(P_1) \approx 0.16728752, \phi(P_2) \approx 0.019066499, \phi(P_3) \approx 0.069180092.$$

Using *Apecs* we computed

$$\hat{h}(P_1) \approx 1.6247112, \hat{h}(P_2) \approx 5.4762626, \hat{h}(P_3) \approx 2.9083116,$$

and $\hat{h}(R_0) = 0$.

Then, by the definition of the A_i 's, we see that we can take

$$A_0 = 27.70, A_1 = A_2 = A_3 = 19.07, \mathcal{E} = e.$$

This leads to

$$c_4 = 2 \cdot 10^{36} \left(\frac{2}{e}\right)^{32} 5^{104} \prod_{i=0}^3 A_i < 1.031 \times 10^{110}.$$

With $t_0 = 2$, $c_5 = 1$, and $c_6 = 1 + h_E$ in (16), we may choose

$$c_7 = 2.824, c_8 = 20.73.$$

In the notation of (2) and (3), we have

$$u = 1, v = -\frac{337}{3}, w = z = 0.$$

Moreover,

$$\gamma = -\frac{2}{3} \cdot 337, \quad \gamma' = \frac{1}{3} \cdot 337 + 337i, \quad \gamma'' = \overline{\gamma'},$$

which implies, by Inequality 2,

$$c_2 = \frac{2}{3} \cdot 337\sqrt{10}.$$

Further, $c_1 \approx 0.67736605$, and $c_3 \approx 5.1930490$, where we have chosen the global minimal Weierstraß model

$$Y^2 = X^3 + X^2 + 75713X + 28375425$$

for the computation of c_3 . We choose

$$c_1 = 0.6773, \quad c_3 = 5.194.$$

Now (16) immediately implies that

$$M < 4.907 \cdot 10^{59}, \tag{26}$$

provided that $X(P) \geq 711 = X_0 = \lfloor \max\{c_2, u^2\gamma + v, v\} \rfloor + 1$. In view of (12), we may take

$$K_1 = 2318 > \frac{4\sqrt{2}}{\omega} \exp(c_3), \quad K_2 = 0.6773,$$

and, because of (26),

$$K_3 = 4.907 \cdot 10^{59}.$$

Choosing

$$K_0 = 10^{245},$$

which is somewhat larger than $(8\sqrt{6}K_3)^4$, means that we must compute $\phi(P_i)$ for $i = 1, 2, 3$ with a precision of 245 decimal digits. Applying the same implementation of the LLL-algorithm as before, we get a reduced basis $\{\mathbf{b}_1, \dots, \mathbf{b}_4\}$ with

$$\mathbf{b}_1 = (-1.534 \dots \times 10^{61}, 3.143 \dots \times 10^{60}, -2.629 \dots \times 10^{60}, -3.680 \dots \times 10^{60}),$$

from which we see that

$$\|\mathbf{b}_1\| > 1.627 \times 10^{61} > 8\sqrt{6}K_3.$$

Therefore, by the Proposition, $M \leq 25$. Repeating the process with K_1, K_2 as above and $K_3 = 25, K_0 = 10^{12}$, the LLL-algorithm gives a reduced basis with

$$\mathbf{b}_1 = (234, -445, 135, -322).$$

Consequently,

$$\|\mathbf{b}_1\| = \sqrt{374690} > 8\sqrt{6}K_3,$$

so that our Proposition yields the new bound

$$M \leq 6.$$

A direct computer search reveals that the only points

$$P = m_1P_1 + m_2P_2 + m_3P_3 + \epsilon T, \quad 0 \leq m_1 \leq 6, \quad -6 \leq m_2, m_3 \leq 6, \quad \epsilon \in \{0, 1\}$$

with integral $X(P) \geq 711$ are those given in the following table

m_1	m_2	m_3	ϵ	$X(P)$	$Y(P)$
0	-1	0	0	56784	-13571615
0	1	0	0	56784	13571615
2	0	1	1	2113	-105910

A direct search with `Apecs` for integral points P on (25) with $X(P) < 711$ reveals no points other than $(-337, 0)$ and $(-287, \pm 3130)$ and this confirms the claim of Example 2.

Appendix: An explicit lower bound for linear forms in elliptic logarithms

We recall the following facts:

- The *absolute logarithmic height* of $(q_1, \dots, q_n) \in \mathbb{Q}^n$ is given by:

$$h(q_1, \dots, q_n) = \sum_p \log \max\{1, |q_1|_p, \dots, |q_n|_p\},$$

where p runs through all primes, including the “infinite” one ($|x|_\infty = |x|$, the usual absolute value). If $n = 1$ and $q_1 = a/b$ with $\gcd(a, b) = 1$, then it is straightforward to check that $h(q_1) = \log \max\{|a|, |b|\}$.

- To any pair of complex numbers A, B such that $\Delta := A^3 - 27B^2 \neq 0$, a so-called Weierstraß \wp -function corresponds with invariants $g_2 = A$, $g_3 = B$. This function \wp of a single complex variable is doubly periodic and has one second-order pole in a period parallelogram. Further, \wp satisfies the differential equation $\wp'(z)^2 = 4\wp(z)^3 - A\wp(z) - B$ and $x = \wp(z)$, $y =$

$\wp'(z)$ gives a parameterization over \mathbb{C} of the elliptic curve with Weierstraß equation

$$y^2 = 4x^3 - Ax - B =: f_1(x), \quad (27)$$

where z runs through all values of a fundamental parallelogram of the period lattice.

- The fundamental periods ω_1 and ω_2 of the function \wp may be expressed by the following definite integrals (see [AS, 18.7.4 and 18.7.5 on p. 641]):

If $\Delta > 0$, then $f_1(x)$ has three real zeros $e_1 > e_2 > e_3$, and

$$\frac{\omega_1}{2} = \int_{e_1}^{\infty} \frac{dt}{\sqrt{f_1(t)}}, \quad \frac{\omega_2}{2} = i \int_{-\infty}^{e_3} \frac{dt}{\sqrt{|f_1(t)|}}.$$

A fast and convenient method for computing the periods numerically is provided by the *Arithmetic–Geometric Mean (AGM)*, see [C]. If the AGM of two positive reals a and b is denoted by $M(a, b)$, then (see [BM, 2.1, in particular (10) and (11)]):

$$\omega_1 = \frac{\pi}{M(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}, \quad \omega_2 = \frac{\pi i}{M(\sqrt{e_1 - e_3}, \sqrt{e_2 - e_3})}. \quad (28)$$

If $\Delta < 0$, then $f_1(x)$ has one real root e_1 and a pair of complex conjugate roots e_2 and $e_3 = \bar{e}_2$, and

$$\omega_1 = \int_{e_1}^{\infty} \frac{dt}{\sqrt{f_1(t)}} + i \int_{-\infty}^{e_1} \frac{dt}{\sqrt{|f_1(t)|}}, \quad \omega_2 = \bar{\omega}_1.$$

Again, as in the case of a positive discriminant, more convenient formulas exist for the computation of the periods. Consider the curve

$$Y^2 = 4X^3 - 4(15e_1^2 - A)X - 2(7e_1A + 11B). \quad (29)$$

This curve and (27) are 2-isogenous. Consequently, if Ω_1, Ω_2 is a pair of fundamental periods for the Weierstraß function associated with (29), then $\omega_1 = \Omega_1 + \Omega_2$, $\omega_2 = \Omega_1 - \Omega_2$ can be taken as a pair of fundamental periods for the Weierstraß function \wp associated with (27). But the right-hand-side of (29) has the three real roots

$$e_1 + \sqrt{12e_1^2 - A} > -2e_1 > e_1 - \sqrt{12e_1^2 - A}.$$

Therefore, like in the case of a positive discriminant, the periods Ω_1, Ω_2 —and hence ω_1, ω_2 too—can be computed numerically by the AGM method. Finally, the pair of fundamental periods ω_1, ω_2 may be chosen such that $\tau = \omega_2/\omega_1$ satisfies

$$|\tau| \geq 1, \quad \Im\tau > 0, \quad -\frac{1}{2} < \Re\tau \leq \frac{1}{2} \quad \text{with} \quad \Re\tau \geq 0 \quad \text{if} \quad |\tau| = 1. \quad (30)$$

Consider the equation

$$y^2 = x^3 + ax + b =: f(x) \quad \text{with} \quad a, b \in \mathbb{Q}, \quad (31)$$

and let \wp be the Weierstraß function corresponding to (31), i.e. the one with invariants $g_2 = -a/4$, $g_3 = -b/16$. Note that now $x = 4\wp(z)$, $y = 4\wp'(z)$ gives a parameterization over \mathbb{C} of the elliptic curve E defined by (31).

Matching up the notation of this Appendix with the rest of the paper, we get

$$f_1(x) = 4x^3 + \frac{a}{4}x + \frac{b}{16}, \quad \gamma = 4e_1, \quad \gamma' = 4e_2, \quad \gamma'' = 4e_3,$$

where γ is the largest (or the only) real zero, and γ' , γ'' are the remaining zeros of $f(x)$. In view of the foregoing discussion on the periods, it immediately follows that a pair of fundamental periods is given by

$$\omega_1 = \frac{2\pi}{M(\sqrt{\gamma - \gamma''}, \sqrt{\gamma - \gamma'})}, \quad \omega_2 = \frac{2\pi i}{M(\sqrt{\gamma - \gamma''}, \sqrt{\gamma' - \gamma''})}$$

in the case of three real roots $\gamma > \gamma' > \gamma''$, and by

$$\omega_1 = \Omega_1 + \Omega_2, \quad \omega_2 = \Omega_1 - \Omega_2, \quad (32)$$

with

$$\Omega_1 = \frac{\pi}{M\left(\sqrt[4]{3\gamma^2 + a}, \frac{1}{2}\sqrt{3\gamma + 2\sqrt{3\gamma^2 + a}}\right)},$$

$$\Omega_2 = \frac{\pi i}{M\left(\sqrt[4]{3\gamma^2 + a}, \frac{1}{2}\sqrt{-3\gamma + 2\sqrt{3\gamma^2 + a}}\right)},$$

in the case of a single real root γ .

Let $u_0, \dots, u_r \in \mathbb{C}$ be such that, for every $i = 0, \dots, r$, $R_i = (4\wp(u_i), 4\wp'(u_i)) \in E(\mathbb{Q}) \cup \{O\}$ on (31)—note that $R_i = O$ means that u_i is a pole of \wp .

Let $j_E = 2^8 3^3 a^3 / (4a^3 + 27b^2)$ be the j -invariant of E and define

$$h_E = \max\{1, h(a/4, b/16), h(j_E)\}.$$

Let ω_1, ω_2 be a pair of fundamental periods for \wp with $\tau = \omega_2/\omega_1$ satisfying (30). For every $i = 0, \dots, r$, consider a positive number A_i such that

$$A_i \geq \max\left\{\hat{h}(R_i), h_E, \frac{3\pi u_i^2}{|\omega_1|^2 \Im \tau}\right\},$$

where \hat{h} denotes the usual Néron-Tate or canonical height function. Further, consider a number \mathcal{E} satisfying

$$e \leq \mathcal{E} \leq \min_{i=0, \dots, r} \left\{ \frac{e|\omega_1|\sqrt{A_i \Im \tau}}{|u_i|\sqrt{3\pi}} \right\},$$

and finally, let L be the linear form

$$L = \frac{b_0}{t}u_0 + b_1u_1 + \cdots + b_ru_r,$$

where $t, b_0, b_1, \dots, b_r \in \mathbb{Z}$ and $t > 0$. Also let B be a positive integer such that

$$B \geq \max\{A_0, \dots, A_r, t, |b_0|, |b_1|, \dots, |b_r|, 16\}.$$

The following theorem is a special case of [D, Théorème 2.1].

David's Theorem . *If $L \neq 0$, then*

$$|L| \geq \exp(-c_4(\log B + \log \mathcal{E})(\log \log B + \log \mathcal{E} + h_E)^{r+2}),$$

where

$$c_4 = 2 \cdot 10^{7r+15} \left(\frac{2}{e}\right)^{2(r+1)^2} (r+2)^{4r^2+18r+14} (\log \mathcal{E})^{-2r-3} \prod_{i=0}^r A_i.$$

References

- [AS] MILTON ABRAMOWITZ and IRENE STEGUN (eds.), “Handbook of Mathematical Functions”. Dover Publ., New York 1964.
- [BM] J.-B. BOST and J.-F. MESTRE, Moyenne Arithmético-géométrique et Périodes des Courbes de Genre 1 et 2, *Gazette de Mathématiciens*, S.M.F., Octobre 1988.
- [Br] ANDREW BREMNER, An Equation of Mordell, *Math. Comp.* **29** (1975), 925–928.
- [C] D.A. COX, The Arithmetic-Geometric Mean of Gauss, *Enseign. Math.* **30** (1984), 275–330.
- [D] S. DAVID, Minorations de formes linéaires de logarithmes elliptiques, *Publ. Math. de l'Un. Pierre et Marie Curie* no. 106, Problèmes diophantiens 1991–1992, exposé no. 3.
- [H] N. HIRATA-KOHNO, Formes linéaires de logarithmes de points algébriques sur les groupes algébriques, *Invent. Math.* **104** (1991), 401–433.
- [La] S. LANG, “Elliptic Curves; Diophantine Analysis”, Grundlehren der mathematischen Wissenschaften **231**, Springer-Verlag, Berlin/Heidelberg 1978.

- [LLL] A.K. LENSTRA, H.W. LENSTRA and L. LOVÁSZ, Factoring Polynomials with Rational Coefficients, *Math. Ann.* **261** (1982), 515–534.
- [Lj] W. LJUNGGREN, A diophantine problem, *J. London Math. Soc.* (2) **3** (1971), 385–391.
- [Ma] D.W. MASSER, “Elliptic Functions and Transcendence”, Lecture Notes in Mathematics **437**, Springer-Verlag, Berlin/Heidelberg 1975.
- [Mo] L.J. MORDELL, “Diophantine Equations”, Pure and Applied Mathematics Series **30**, Academic Press, London and New York 1969.
- [S1] J.H. SILVERMAN, “The Arithmetic of Elliptic Curves”, Graduate Texts in Mathematics **106**, Springer-Verlag, New York 1986.
- [S2] J.H. SILVERMAN, Computing Heights on Elliptic Curves, *Math. Comp.* **51** (1988), 339–358.
- [S3] J.H. SILVERMAN, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **55** (1990), 723–743.
- [STo] ROEL J. STROEKER and JAAP TOP, On the equation $Y^2 = (X + p)(X^2 + p^2)$, *Rocky Mount. J. Math.* (1994), to appear.
- [STz] R.J. STROEKER and N. TZANAKIS, On the Application of Skolem’s p-adic Method to the Solution of Thue Equations, *J. Number Th.* **29**(2) (1988), 166–195.
- [TdW] N. TZANAKIS and B.M.M. DE WEGER, On the Practical Solution of the Thue Equation, *J. Number Th.* **31**(2) (1989), 99–132.
- [dW] B.M.M. DE WEGER, “Algorithms for Diophantine Equations”, CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam 1989.
- [WW] E.T. WHITTAKER and G.N. WATSON, “A Course of Modern Analysis” (4th ed.), Cambridge University Press, New York 1978.
- [Wu] G. WÜSTHOLZ, Recent Progress in Transcendence Theory, in: “Number Theory, Noordwijkerhout 1983”, Lecture Notes in Mathematics **1068**, Springer-Verlag, Berlin/Heidelberg 1984, 280–296.
- [Z] D. ZAGIER, Large Integral Points on Elliptic Curves, *Math. Comp.* **48** (1987), 425–436.