ACTA ARITHMETICA
LXXV.2 (1996)

Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations

by

N. Tzanakis (Iraklion)

1. Introduction. In a recently published paper [ST], R. J. Stroeker and the author describe in detail—with examples included—a general method for computing all integer solutions of a Weierstrass equation, which defines an elliptic curve over $\mathbb{Q}$. A little later, J. Gebel, A. Pethő and H. G. Zimmer worked independently on similar lines and solved a number of impressive numerical examples (see [GPZ]); for some history of the main ideas underlying that method see the introduction in [ST]. The main advantage of the method, which combines the *Arithmetic of Elliptic Curves* with the Theory of *Linear Forms in Elliptic Logarithms*, is that it is very easily—almost mechanically—applicable, once one knows a Mordell–Weil basis for the elliptic curve associated with the given equation. In this way, one can solve, with reasonable effort, many elliptic diophantine equations that are "of the same type"; for an interesting application see [Str], where fifty elliptic equations are solved. We note that the ineffective part of the method (i.e. the computation of a Mordell–Weil basis) is completely independent of all the remaining steps; this helps a great deal in organizing the computational work in practice.

In this paper we extend the aforementioned method to the class of *quartic elliptic equations*, i.e. we describe a general practical method for computing explicitly all integral solutions of equations of the form $V^2 = Q(U)$, where $Q(U) \in \mathbb{Z}[U]$ is a quartic polynomial with non-zero discriminant. Such equations have a long history; see Chapter XXII of [Di] and sections D24 of [LV] and [G]. However, very few results concerning such equations are of a general character and these deal with special types of quartic elliptic equations (like, for example, $x^4 - Dy^2 = 1$). In most cases, specific numerical examples are solved completely by clever but often very laborious *ad hoc* arguments; typical examples are the papers [L1], [L2] and [L3] by W. Ljunggren and [B] by R. Bumby. The method we propose in the present paper has a general character; it is reasonable therefore to apply it to equations which are already well known for the difficulty of their solution, like, for example, those mentioned above. This we do in Section 6 (Examples 2 through 7). The uniformity and simplicity of the way they are solved by the method of the present paper, compared to the *ad hoc* elaborate ways found in older literature, is apparent. It is worth noticing that these "historic" examples are associated with elliptic curves of rank 1 or 2 with an easily found Mordell–Weil basis. Example 1 has been chosen by the author for illustrating the method in more detail.

As the reader will see in the next section, the proposed method consists in finding all points $m_1P_1 + \ldots + m_rP_r$—with $P_1, \ldots, P_r$ a Mordell–Weil basis for the elliptic curve—that have integral coordinates. This is done in three steps: (1) One finds an upper bound for $M = \max_{1\le i\le r} |m_i|$ by using an explicit result of S. David [Da]. (2) This upper bound is reduced by using the LLL-basis reduction algorithm. (3) All points $P_1, \ldots, P_r$ are checked in that reduced range of M. In case of equations associated with elliptic curves of rank ≥ 4 (say), the necessary computations might be quite heavy: First, the computation of the Mordell–Weil basis is then far from easy. Second, the calculations needed for the reduction of the large upper bound of M depend heavily on the rank r. Third, to check all points $m_1P_1 + \ldots + m_rP_r$ in the range $M \le$ small constant is not trivial if r is large ([1]). In this paper we do not deal with the solution of such complicated examples, a task that will be the subject of a future work. J. Top [T2] has already constructed interesting examples of quartic equations corresponding to elliptic curves of high rank; we have good reasons to believe that, apart from the much heavier computations that will be needed, the method of the present paper will work for these examples too.

2. Preliminaries. We are interested in computing explicitly all solutions $(U, V) \in \mathbb{Z} \times \mathbb{Z}$ of an equation $V^2 = Q(U)$, where Q is a quartic polynomial with rational integer coefficients and non-zero discriminant. We suppose that this equation has at least one rational solution (u_0, v_0). Let $u_0 = m/n$, with m, n relatively prime integers. For any integer solution (U, V) of $V^2 = Q(U)$ we put $U = (U_1 + m)/n$, where U_1 is an integer. Then our equation is transformed into an equation $V_1^2 = Q_1(U_1)$, where Q_1 is a quartic polynomial with integer coefficients and constant term which is a perfect square ($V_1 = n^2V$). Thus (omitting the subscripts 1), our initial

([1]) Analogous difficulties arise also when we are considering cubic elliptic equations as in [ST] and [GPZ].

problem is reduced to solving in integers the following type of equations:

(1) $V^2 = Q(U) := aU^4 + bU^3 + cU^2 + dU + e^2, \quad a,b,c,d,e \in \mathbb{Z},\ a,e>0.$

This equation defines an elliptic curve $E/\mathbb{Q}$ and by an explicit birational transformation we obtain a Weierstrass model $W(X,Y) = 0$ of E, with coefficients

$$a_1 = \frac{d}{e}, \quad a_2 = \frac{4e^2c - d^2}{4e^2}, \quad a_3 = 2eb, \quad a_4 = -4e^2a, \quad a_6 = ad^2 - 4e^2ac;$$

see [Cn]. The transformation and its inverse can be performed e.g. by Ian Connell's Apecs, based on MapleV. Finally, the transformation

$$X = x - \frac{c}{3}, \quad Y = \sigma y - \frac{d}{2e}x + \frac{cd}{6e} - eb, \quad \sigma \in \{+1,-1\},$$

transforms $W(X,Y) = 0$ into

$$y^2 = q(x) := x^3 + Ax + B,$$
$$A = -\frac{1}{3}c^2 + bd - 4e^2a, \quad B = \frac{2}{27}c^3 - \frac{1}{3}bcd - \frac{8}{3}e^2ac + e^2b^2 + ad^2.$$

For any point $P \in E$, we will denote its coordinates by

$$(U(P),V(P)), \quad (X(P),Y(P)), \quad (x(P),y(P)),$$

depending on which model of E we refer to.

We will need to integrate the differential form dU/V along an infinite path on the real axis. Since dU/V and dx/y are differential forms on the same elliptic curve, we expect that they differ multiplicatively by a rational function. An actual calculation shows that $dU/V = -\sigma dx/y$, but we need to know how the integration limits of the two integrals are related; this is what we do below.

It is easy to prove that at least one of the two quantities $d\sqrt{a} + eb$ and $8e^3\sqrt{a} + 4e^2c - d^2$ is non-zero. We put

$$\sigma = \begin{cases} \operatorname{sgn}(d\sqrt{a} + eb) & \text{if } d\sqrt{a} + eb \neq 0, \\ \operatorname{sgn}(8e^3\sqrt{a} + 4e^2c - d^2) & \text{if } d\sqrt{a} + eb = 0, \end{cases} \qquad x_0 = 2e\sqrt{a} + c/3.$$

For $u > 0$ sufficiently large, so that $Q(u) > 0$, we define the functions

$$\mathcal{F}^*(u) = \frac{2e\sqrt{Q(u)} + du + 2e^2}{u^2}, \qquad f^*(u) = \mathcal{F}^*(u) + \frac{c}{3}.$$

We can find explicitly a positive parameter u_0 such that $Q(u) > 0$ for $u > u_0$ and $\mathcal{F}^*$ is strictly monotonic in the interval $(u_0, +\infty)$ (decreasing if $\sigma = 1$, increasing if $\sigma = -1$) and $\mathcal{F}^*((u_0,+\infty))$ does not contain the two numbers $-2e\sqrt{a}$ and $(d^2 - 4e^2c)/(4e^2)$. We also note that $\lim_{u\to+\infty} = 2e\sqrt{a}$ and $\mathcal{F}^*((u_0,+\infty))$ is the interval with endpoints $\mathcal{F}^*(u_0)$ and $2e\sqrt{a}$.

Proposition 1. *Let $U > u_0$. Then*

$$\int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \sigma \int_{x_0}^{f^*(U)} \frac{dx}{\sqrt{x^3 + Ax + B}}.$$

We omit the proof, because it is somewhat technical and without any theoretical interest.

3. The elliptic integral as a linear form in elliptic logarithms. Let U be any real number $> u_0$, where u_0 is as in end of Section 2. In this section we express the integral

$$\int_U^{+\infty} \frac{du}{\sqrt{Q(u)}}, \qquad U > u_0, \tag{2}$$

as a linear form in the ϕ-values of certain fixed points on E. Here ϕ denotes the group isomorphism

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

where $E_0(\mathbb{R})$ is the infinite component of the model $y^2 = x^3 + Ax + B$, defined in [Z], p. 429, or in the introduction of [ST]. Let us denote by ω the fundamental real period of the Weierstrass $\wp$ function associated with $y^2 = q(x)$ (for the practical computation of ω see Section 7). For any point $P \in E_0(\mathbb{R})$ we have by [Z],

$$\omega\phi(P) \equiv \pm \int_{x(P)}^{+\infty} \frac{dt}{\sqrt{q(t)}} \pmod 1.$$

Now we make correspond to U the point $P \in E$ defined by

$$x(P) = f^*(U), \qquad y(P) \geq 0.$$

Note that if both U and $\sqrt{Q(U)}$ are rationals, then, in view of the birational transformation between the models $V^2 = Q(U)$ and $y^2 = q(x)$, we see that $x(P)$ and $y(P)$ are rationals. If P is on $E_0(\mathbb{R})$ then, by [Z], p. 429, or the introduction of [ST], we can take (by identifying $\mathbb{R}/\mathbb{Z}$ with the interval $[0, 1)$ equipped with the addition mod1)

$$\omega\phi(P) = \int_{x(P)}^{+\infty} \frac{dt}{\sqrt{q(t)}}.$$

By Proposition 1 the integral in (2), which corresponds to the particular value U we consider, is, up to sign, equal to $\omega\phi(P)$. It may happen, however, that P does not belong to the infinite component $E_0(\mathbb{R})$. In this case, there is no direct relation between the integral in (2) and $\phi(P)$. At this point, a critical role is played by the position of x_0 relative to the roots e_1, e_2, e_3 of $q(x)$. Throughout this paper we denote by e_1 the real root of $q(x)$ if it has only one; in case of three real roots we assume $e_1 > e_2 > e_3$. It is not difficult to prove the following fact:

If $d\sqrt{a}+eb \neq 0$, *then either* $x_0 > e_1$ *or* $x_0 \in (e_3, e_2)$ (*this interval should be understood as the empty set if* $e_2, e_3 \notin \mathbb{R}$). *If* $d\sqrt{a}+eb = 0$, *then* $x_0 = e_1$ *or* e_2, *depending on whether* $\sigma = +1$ (*if* $e_2, e_3 \notin \mathbb{R}$ *this is always the case*) *or* -1, *respectively.*

Another fact is the following:

There is an explicit positive constant U_0 *such that*

$$U > U_0 \Rightarrow x(P) \in \begin{cases} (e_1, +\infty) & \text{if } x_0 \geq e_1, \\ (e_3, e_2) & \text{otherwise.} \end{cases}$$

Note that the complementary case to $x_0 \geq e_1$ is: e_1, e_2, e_3 are reals—hence $e_1 > e_2 > e_3$—and $x_0 \in [e_3, e_2]$. Below we describe how we can calculate a value for U_0. First, we consider the function

$$\mathcal{F}(X) = \frac{4e^2X + 4e^2c - d^2}{-dX - 2e^2b + \sigma e\sqrt{4X^3 + b_2X^2 + 2b_4X + b_6}},$$

defined on the interval with endpoints $\mathcal{F}^*(u_0)$ and $2e\sqrt{a}$; here b_2, b_4, b_6 have their usual meaning in connection with the parameters $a_1, \ldots, a_6$ of the Weierstrass model given at the beginning of Section 2. It can be proved that the functions $\mathcal{F}$ and $\mathcal{F}^*$ are inverse to each other. The following two facts can be proved. We omit their proof, as it is merely technical and without any theoretical interest.

Let $x_0 \geq e_1$. *Put* $e_1' = e_1$ *if* $e_1 - c/3$ *is not a root of the denominator of* $\mathcal{F}$ *and* $e_1' = e_1 + \varepsilon$, *where the "small" positive number* ε *can be chosen arbitrarily*, *otherwise. Put*

$$U_0 := \max(u_0, \mathcal{F}(e_1' - c/3))$$

and let $U > U_0$. *Then*, *for the point* $P \in E$ *which*, *according to the beginning of this section*, *corresponds to* U, *we have* $x(P) > e_1$.

Let $e_1 > e_2 > e_3$. *Let* $x_0 \in (e_3, e_2]$. *Put* $e_2' = e_2$ *if* $e_2 - c/3$ *is not a root of the denominator of* $\mathcal{F}$ *and* $e_2' = e_2 - \varepsilon_2$, *where* ε_2 *is a "small" positive number*, *otherwise*; *similarly*, *put* $e_3' = e_3$ *if* $e_3 - c/3$ *is not a root of the denominator of* $\mathcal{F}$ *and* $e_3' = e_3 + \varepsilon_3$, *where* ε_3 *is a "small" positive number*, *otherwise. The* ε*'s can be chosen arbitrarily*, *but in such a way that* $e_3 \leq e_3' < e_2' \leq e_2$. *Let*

$$U > U_0 := \max(u_0, \mathcal{F}(e_2' - c/3), \mathcal{F}(e_3' - c/3)).$$

Then, *for the point* $P \in E$ *corresponding to* U, *we have* $x(P) \in (e_3, e_2)$.

Remark. It is easy to see that, for $i = 1, 2, 3$, $e_i - c/3$ is a root of the denominator of $\mathcal{F}$ if $de_i = cd/3 - 2e^2b$.

Let now $U > U_0$ and denote by P the point on E which corresponds to U.

First, suppose that $eb + d\sqrt{a} \neq 0$. According to the above discussion, either $x_0 > e_1$ or $e_2, e_3 \in \mathbb{R}$ and $x_0 \in (e_3, e_2)$. Moreover, in the first case we have $x(P) > e_1$, so that we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{x_0}^{+\infty} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)}^{+\infty} \frac{dx}{\sqrt{q(x)}} \tag{3}$$

and in the second case we have $x(P) \in (e_3, e_2)$, so that we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{x_0}^{e_2} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)}^{e_2} \frac{dx}{\sqrt{q(x)}} = \int_{x_0'}^{+\infty} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)'}^{+\infty} \frac{dx}{\sqrt{q(x)}}. \tag{4}$$

Here and in the sequel, in case that e_1, e_2, e_3 are reals, we put

$$X' = e_2 + \frac{(e_1 - e_2)(e_2 - e_3)}{e_2 - X},$$

for every $X \in \mathbb{R}$, $X \neq e_2$; hence, if $X \in (e_3, e_2)$, then $X' > e_1$ and

$$\int_{X}^{e_2} \frac{dx}{\sqrt{q(x)}} = \int_{X'}^{+\infty} \frac{dx}{\sqrt{q(x)}}.$$

The last relation was used in the rightmost side of (4).

Next, suppose that $be + d\sqrt{a} = 0$. According to our previous discussion, either $\sigma = 1$ and $x_0 = e_1$ or $e_2, e_3 \in \mathbb{R}$ and $\sigma = -1$ and $x_0 = e_2$. In the first case, $x(P) > e_1$, so that we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{e_1}^{+\infty} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)}^{+\infty} \frac{dx}{\sqrt{q(x)}}; \tag{5}$$

in the second case, $x(P) \in (e_3, e_2)$ and we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{e_2}^{x(P)} \frac{dx}{\sqrt{q(x)}} = -\int_{x(P)'}^{+\infty} \frac{dx}{\sqrt{q(x)}}. \tag{6}$$

Now we express the integrals on the left-hand sides of (3)–(6) in terms of ϕ-values and ω. In case $e_2, e_3 \in \mathbb{R}$, we denote by Q_2 the point with $x(Q_2) = e_2$, $y(Q_2) = 0$, and for any point $\Pi \in E$, we put $\Pi' = \Pi + Q_2$. Observe that

$$y(\Pi') \geq 0 \Leftrightarrow y(\Pi) \geq 0 \quad \text{and} \quad x(\Pi') = x(\Pi)'.$$

The last relation permits us to replace the lower limits $x(P)'$ of the integrals in (4) and (6) by $x(P')$. Observe also that, if $x(\Pi) \in (e_3, e_2)$, then $\Pi' \in$

$E_0(\mathbb{R})$. Finally, we denote by P_0 the point with $x(P_0) = x_0, y(P_0) = \sigma(be + d\sqrt{a})$.

By Proposition 1, the definition of ϕ and the fact that $y(P) \geq 0$, relations (3)–(6) imply respectively:

• If either $e_2, e_3 \notin \mathbb{R}$ or $e_2, e_3 \in \mathbb{R}$ and $x_0 > e_1$:

$$\frac{1}{\omega} \int\limits_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \sigma(\phi(P_0) - \phi(P)). \tag{7}$$

• If $e_2, e_3 \in \mathbb{R}$ and $x_0 \in (e_3, e_2)$:

$$\frac{1}{\omega} \int\limits_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \sigma(\phi(P_0') - \phi(P')). \tag{8}$$

• If $e_2, e_3 \in \mathbb{R}$ and $x_0 = e_1$:

$$\frac{1}{\omega} \int\limits_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \frac{1}{2} - \phi(P). \tag{9}$$

• If $e_2, e_3 \in \mathbb{R}$ and $x_0 = e_2$:

$$\frac{1}{\omega} \int\limits_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \phi(P'). \tag{10}$$

Consider now a basis $P_1, \ldots, P_r$ for the free part of the group $E(\mathbb{Q})$, and for every $i = 1, \ldots, r$ put

$$R_i = \begin{cases} P_i & \text{if } P_i \in E_0(\mathbb{R}), \\ P_i' & \text{otherwise.} \end{cases}$$

Note that $R_i \in E_0(\mathbb{R})$ (although, in general, $R_i \notin E_0(\mathbb{Q})$), so that $\phi(R_i)$ is defined. More precisely, $R_i \in E_0(\overline{\mathbb{Q}})$ and this fact plays an important role below.

Let $U \in \mathbb{Z}$, $U > 0$, be such that $\sqrt{Q(U)} \in \mathbb{Z}$ and let P be the point which corresponds to U, as explained at the beginning of this section. Since all such U in the interval $[0, U_0]$ can be easily found, we may assume that $U > U_0$. We write

$$P = m_1 P_1 + \ldots + m_r P_r + T, \tag{11}$$

where $m_1, \ldots, m_r$ are integers and T is a torsion point of E. In order to find all integers U as above, it suffices to find a "small" upper bound for

$$M = \max\{|m_1|, \ldots, |m_r|\}.$$

We note here that the assumption $U > 0$ is not actually a restriction. Indeed, for the solution of (1) with negative U, it suffices to solve

$$V^2 = aU^4 - bU^3 + cU^2 - dU + e^2, \qquad U > 0. \tag{12}$$

Therefore, when we calculate the various constants which result in an upper bound for M (these are functions of a, b, c, d, e), we must also calculate the corresponding constants for a, $-b$, c, $-d$, e and consider in each case the worst value.

In view of the definition of the R_i's and the relation $2 \cdot Q_2 = \mathcal{O}$, relation (11) implies that

$$\text{either } P \text{ or } P' = m_1 R_1 + \ldots + m_r R_r + T_0,$$

where T_0 is a torsion point belonging to $E_0(\mathbb{R})$. Then,

$$\text{either } \phi(P) \text{ or } \phi(P') = m_1\phi(R_1) + \ldots + m_r\phi(R_r) + s/t + m_0;$$

here we put $s/t = \phi(T_0)$, $s, t \in \mathbb{Z}$, $0 \le s < t$ and $t \le 12$ by Mazur's theorem. Also, m_0 is an integer with absolute value not exceeding $rM + 1$, since the ϕ-values belong to the interval $[0, 1)$. Going back to (7)–(10) and replacing, if necessary, the m_i's by their opposites, we are led to the following relations:

• If either $e_2, e_3 \notin \mathbb{R}$ or $e_2, e_3 \in \mathbb{R}$ and $x_0 > e_1$:

$$\frac{\sigma}{\omega} \int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \left(m_0 - \frac{s}{t}\right) + \phi(P_0) + m_1\phi(R_1) + \ldots + m_r\phi(R_r). \tag{13}$$

• If $e_2, e_3 \in \mathbb{R}$ and $x_0 \in (e_3, e_2)$:

$$\frac{\sigma}{\omega} \int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \left(m_0 - \frac{s}{t}\right) + \phi(P_0') + m_1\phi(R_1) + \ldots + m_r\phi(R_r). \tag{14}$$

• If $e_2, e_3 \in \mathbb{R}$ and $x_0 = e_1$:

$$\frac{1}{\omega} \int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \left(m_0 - \frac{s}{t} + \frac{1}{2}\right) + m_1\phi(R_1) + \ldots + m_r\phi(R_r). \tag{15}$$

• If $e_2, e_3 \in \mathbb{R}$ and $x_0 = e_2$:

$$\frac{1}{\omega} \int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = \left(m_0 + \frac{s}{t}\right) + m_1\phi(R_1) + \ldots + m_r\phi(R_r). \tag{16}$$

Let $\wp$ denote the Weierstrass function associated with the equation $y^2 = q(x)$. By the definition of the function ϕ, we have, for any point Π on $E_0(\mathbb{R})$, $\wp(\omega\phi(\Pi)) = x(\Pi)$, hence $\omega\phi(\Pi)$ is the *elliptic logarithm* of either Π or of $-\Pi$; also, ω is the elliptic logarithm of the point $\mathcal{O}$. It follows that, on multiplying by ω the relations (13)–(16), we express the left-hand side integrals as non-zero linear forms in elliptic logarithms of points belonging to $E_0(\overline{\mathbb{Q}})$.

Remark. In case of (13) (respectively (14)), if $\phi(P_0)$ (respectively $\phi(P_0')$) is linearly dependent on $\phi(R_1), \ldots, \phi(R_r)$ over $\mathbb{Q}$ (see e.g. Examples 1–4 in Section 6), the term $\phi(P_0)$ (respectively $\phi(P_0')$) can be removed, at the cost of a slight change of the m_i's and, probably, the appearance in some of the modified m_i's of small (known) denominators. Even in such a case, we can find an upper bound for the (unknown) numerators of the modified m_i's, which is of the form $c'_{12}M + c'_{13}$ and c'_{12}, c'_{13} are trivial to compute explicitly.

4. An upper bound of M. In this section we assume that U is an integer $> U_0$ such that $\sqrt{Q(U)} \in \mathbb{Z}$ and denote by P the point on E that corresponds to U, as explained at the beginning of Section 3. Therefore one of the four relations (13)–(16) holds. In any of these relations, we denote the linear form on the right-hand side by $\Phi(U)$. We intend to compute an upper and a lower bound of $\Phi(U)$ in terms of M and of various explicitly computable positive constants c_i depending on Q and U_0. Then we will combine the two bounds to obtain an upper bound of M.

Obviously, the integral on the left-hand side is positive and we can find for it an upper bound of the form $c_9 U^{-1}$, hence

$$0 < \Phi(U) < \frac{c_9}{\omega}|U|^{-1}. \tag{17}$$

Now, consider any Weierstrass equation with rational integer coefficients defining our elliptic curve E; say, $W(X_1, Y_1) = 0$. The coordinates $X_1(P)$ and $X(P)$, for any point P, are related by an equation of the form $X_1(P) = \alpha^2 X(P) + \beta$, for some rational numbers α and β and since we have, by the definition of P,

$$X(P) = x(P) + \frac{c}{3} = f^*(U) + \frac{c}{3} = \frac{2e\sqrt{Q(U)} + dU + 2e^2}{U^2},$$

and U is an integer, it follows that a non-negative constant c_{10} can be explicitly calculated (2), such that

$$h(X_1(P)) \le c_{10} + 2\log U \quad \text{if } U \text{ is not “very small”}. \tag{18}$$

Here $h(\cdot)$ denotes the Weil height. If we denote by $\widehat{h}(\cdot)$ the Néron–Tate height, then, by applying Theorem 1.1 of J. Silverman [S2], we can easily calculate an explicit positive constant c_{11}, such that

$$\widehat{h}(P) - \tfrac{1}{2}h(X_1(P)) \le c_{11}. \tag{19}$$

Note that the choice of the Weierstrass equation $W(X_1, Y_1) = 0$ is arbitrary (but, as already noted, the coefficients must be rational integers); therefore if we have at our disposal several such equations, we choose the one that implies the smallest value for c_{11}. In the examples that we solve in Section 6,

(2) We remind the reader here that, for the actual calculation of c_9 and c_{10} in a specific numerical example, one has to take into account the comment after relation (12).

we choose the *minimal Weierstrass equation*, computed by Apecs (Laska's algorithm).

By Inequality 1 in Section 3 of [ST], we have $\widehat{h}(P) \geq c_1 M^2$ for some positive constant c_1 (the computation of c_1 is rather easy with the help of Apecs and MapleV, for example; actually, c_1 is the least eigenvalue of the regulator matrix corresponding to the points $P_1, \ldots, P_r$; see the end of Section 2 of [ST]), therefore, by (19),

$$-\tfrac{1}{2} h(X_1(P)) \leq c_{11} - \widehat{h}(P) \leq c_{11} - c_1 M^2$$

and now by (18) and (17),

$$|\omega \Phi(U)| \leq c_9 \exp\left(c_{11} + \tfrac{1}{2} c_{10}\right) \cdot \exp(-c_1 M^2). \tag{20}$$

Now we compute a lower bound of $|\Phi(U)|$ by applying Theorem 2.1 of S. David [Da], as stated in Section 7. As we saw at the end of the previous section, $\omega\Phi(U)$ is a linear form in elliptic logarithms, say,

$$\frac{n_0}{d_0}\omega + \frac{n_1}{d_1}u_1 + \frac{n_2}{d_2}u_2 + \ldots + \frac{n_\nu}{d_\nu}u_\nu.$$

Here, the u's are either of the form $\omega\phi(R_i)$ or $\omega\phi(P_0)$, or $\omega\phi(P_0')$, $\nu = r$ or $r+1$ and the fractions n_i/d_i, in lowest terms, are defined explicitly by means of the m_i's and they differ from them "very little", if at all. We now define

$$N = \max\{|n_0|, |n_1|, \ldots, |n_\nu|\}.$$

Since $|m_0| \leq rM + 1$ and $0 < t \leq t_0$, $0 \leq s < t_0$, where t_0 is the maximal order of torsion points, we easily find explicit constants c_{12}, c_{13} such that

$$N \leq c_{12} M + c_{13}. \tag{21}$$

By David's theorem (see Theorem 5), we have

$$|\omega\Phi(U)| \geq \exp(-c_4(\log N + c_5)(\log\log N + c_6)^{\nu+2}) \tag{22}$$

(the computation of the constants c_4–c_6 is discussed in detail in Section 7). The combination of (20) and (22) gives

$$c_1 M^2 \leq \log c_9 + \tfrac{1}{2} c_{10} + c_{11} + c_4(\log N + c_5)(\log\log N + c_6)^{\nu+2}.$$

In view of (21) and the fact that we may assume $M \geq 16$, this implies

$$M^2 \leq c_1^{-1}\left(\log c_9 + \tfrac{1}{2}c_{10} + c_{11}\right) + c_1^{-1} c_4 (\log M + c_7)(\log\log M + c_8)^{\nu+2}, \tag{23}$$

where

$$c_7 = c_5 + \log c_{12} + \frac{c_{13}}{16 c_{12}}, \qquad c_8 = c_6 + \left(\log c_{12} + \frac{c_{13}}{16 c_{12}}\right) \Big/ \log 16$$

and thus we have gotten the desired upper bound for M.

5. Reduction of the upper bound. In view of inequality (20) and the upper bound obtained from (23) we can write

$$|\Phi| < K_1 \exp(-K_2 M^2), \qquad M < K_3, \tag{24}$$

where we have put, for simplicity in the notation, Φ instead of $\Phi(U)$ and, of course,

$$K_1 = \frac{c_9}{\omega} \exp\left(c_{11} + \frac{c_{10}}{2}\right), \qquad K_2 = c_1$$

and K_3 is "very large". We put

$$\frac{s'}{t'} = \begin{cases} -s/t & \text{in case of (13), (14)}, \\ -s/t + 1/2 & \text{in case of (15)}, \\ s/t & \text{in case of (16)}, \end{cases} \qquad t' > 0,\ \gcd(s', t') = 1.$$

We also put for simplicity in the notation

$$\phi(R_i) = \varrho_i, \qquad i = 1, \ldots, r,$$

and in case of (13) and (14) only,

$$\varrho_0 = \begin{cases} \phi(P_0) & \text{in case of (13)}, \\ \phi(P_0') & \text{in case of (14)}. \end{cases}$$

We distinguish three cases:

Case 1: One of the relations (15) or (16) holds. In this case our linear form is

$$\Phi = m_1 \varrho_1 + \ldots + m_r \varrho_r + (m_0 + s'/t').$$

Case 2: One of the relations (13) or (14) holds and ϱ_0 is *linearly independent* of $\varrho_1, \ldots, \varrho_r$ over $\mathbb{Q}$. In this case our linear form is

$$\Phi = \varrho_0 + m_1 \varrho_1 + \ldots + m_r \varrho_r + (m_0 + s'/t'). \tag{25}$$

Case 3: One of the relations (13) or (14) holds and ϱ_0 is *linearly dependent* on $\varrho_1, \ldots, \varrho_r$ over $\mathbb{Q}$. In this case our linear form is

$$\Phi = \frac{n_0}{d_0} + \frac{n_1}{d_1} \varrho_1 + \ldots + \frac{n_r}{d_r} \varrho_r;$$

here the n_i's are explicit (usually very simple) linear combinations of the m_i's, $\max_{0 \le i \le r} |n_i| \le c_{12} M + c_{13}$ and the d_i's are small integers (usually 1 or 2).

Next, we consider the $(r+1)$-dimensional lattice Γ generated by the columns of the matrix

$$\mathcal{A} = \begin{pmatrix} 1 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ [K_0 \varrho_1] & \cdots & [K_0 \varrho_r] & K_0 \end{pmatrix}$$

($[\cdot]$ means rounding towards zero, i.e. $[\alpha] = \lfloor \alpha \rfloor$ if $\alpha \ge 0$ and $[\alpha] = \lceil \alpha \rceil$ if $\alpha < 0$). Here K_0 is a conveniently chosen integer, somewhat larger than $(2^{r/2} t' K_3 \sqrt{r^2+r})^{r+1}$ (note that t' is, at most, $2t_0$, where $t_0 \le 12$ is the maximal possible order for torsion points of E). We compute an LLL-reduced basis (see [LLL]) $\mathbf{b}_1, \ldots, \mathbf{b}_{r+1}$, using the "integral version" of the LLL-algorithm (which avoids rounding off errors) due to de Weger (see Section 3.5 of [dW]). The propositions of this section imply a reduction of the large upper bound K_3 to something of the size of $(K_2^{-1} \log K_3)^{1/2}$. In Case 1 we apply the following result, proved in Section 5 of [ST].

Proposition 2. *If* $|\mathbf{b}_1| > 2^{r/2} t' K_3 \sqrt{r^2+r}$, *then*

$$M^2 \le K_2^{-1} (\log(K_0 K_1) - \log(\sqrt{t'^{-2} 2^{-r} |\mathbf{b}_1|^2 - r K_3^2} - r K_3)).$$

In Case 3, we apply the following result, the proof of which is essentially identical to that of Proposition 2.

Proposition 3. *Let*

$$d = \operatorname{lcm}(d_0, \ldots, d_r), \qquad \max_{1 \le i \le r} |n_i| \le c'_{12} M + c'_{13}$$

(*note that* $c'_{12} \le c_{12}$ *and* $c'_{13} \le c_{13}$; *cf.* (21)) *and*

$$K_4 = \max_{1 \le i \le r} |d/d_i| \cdot (c'_{12} K_3 + c'_{13}).$$

If $|\mathbf{b}_1| > 2^{r/2} K_4 \sqrt{r^2+r}$, *then*

$$M^2 \le K_2^{-1} (\log(d K_0 K_1) - \log(\sqrt{2^{-r} |\mathbf{b}_1|^2 - r K_4^2} - r K_4)).$$

Finally, in the "non-homogeneous" Case 2 we work as follows: We consider the point

$$\mathbf{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -t'[K_0 \varrho_0] \end{pmatrix},$$

as a point of $\mathbb{R}^{r+1}$ and we express it with respect to the reduced basis of Γ that we have computed. The coordinates $x_1, \ldots, x_{r+1}$ of $\mathbf{x}$ with respect to this basis are given by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{r+1} \end{pmatrix} = \mathcal{B}^{-1} \mathbf{x},$$

where $\mathcal{B}$ denotes the matrix with columns formed by the vectors of the reduced basis. De Weger's version of the LLL-algorithm computes at the same time matrices $\mathcal{U}$ and $\mathcal{V} = (v_{ij})$, such that $\mathcal{B} = \mathcal{A}\mathcal{U}$ and $\mathcal{V} = \mathcal{U}^{-1}$.

In view of the simplicity of the shape of $\mathcal{A}$, we can easily compute the coordinates $x_1, \ldots, x_{r+1}$; indeed,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{r+1} \end{pmatrix} = \mathcal{V}\mathcal{A}^{-1}\mathbf{x} = -\frac{t'[K_0\varrho_0]}{K_0}\begin{pmatrix} v_{1,r+1} \\ \vdots \\ v_{r+1,r+1} \end{pmatrix}.$$

On the other hand, we can compute a lower bound for the distance $d(\mathbf{x}, \Gamma)$ of the point $\mathbf{x}$ from the lattice Γ: By Lemma 3.5 of [dW] we have

$$d(\mathbf{x}, \Gamma) \geq 2^{r/2}\|x_{i_0}\||\mathbf{b}_1|, \tag{26}$$

where $\|\cdot\|$ denotes "distance from the nearest integer" and $i_0 \in \{1, \ldots, r+1\}$ is so chosen that $\|x_{i_0}\|$ be minimal among $\|x_1\|, \ldots, \|x_{r+1}\|$. Next we consider the lattice point

$$\mathbf{y} = \mathcal{A}\begin{pmatrix} t'm_1 \\ \vdots \\ t'm_r \\ t'm_0 + s' \end{pmatrix} = \begin{pmatrix} t'm_1 \\ \vdots \\ t'm_r \\ \lambda_0 \end{pmatrix},$$

where $\lambda_0 = t'm_1[K_0\varrho_1] + \ldots + t'm_r[K_0\varrho_r] + (t'm_0 + s')K_0$. In view of (26) we have

$$2^{r/2}\|x_{i_0}\||\mathbf{b}_1| \leq |\mathbf{y} - \mathbf{x}| = t'^2(m_1^2 + \ldots + m_r^2) + \lambda^2,$$

where $\lambda = t'[K_0\varrho_0] + \lambda_0$, hence, as is easily seen,

$$|\lambda - K_0 t'\Phi| < t'(1 + rM) \leq t'(1 + rK_3).$$

In view of this and (26) we easily see that

$$1 + rK_3 + K_0|\Phi| \geq \sqrt{2^{-r}t'^{-2}\|x_{i_0}\|^2|\mathbf{b}_1|^2 - rK_3^2},$$

which, combined with (24), gives

$$K_0K_1\exp(-K_2M^2) > \sqrt{2^{-r}t'^{-2}\|x_{i_0}\|^2|\mathbf{b}_1|^2 - rK_3^2} - rK_3 - 1.$$

If the right-hand side is a real positive number, we can take logarithms of both sides and obtain thus the following result, which we apply in case Φ is given by (25):

PROPOSITION 4. *If* $\|x_{i_0}\||\mathbf{b}_1| > 2^{r/2}t'\sqrt{(r^2+r)K_3^2 + 2rK_3 + 1}$, *then*

$$M^2 \leq K_2^{-1}(\log(K_0K_1) - \log(\sqrt{t'^{-2}2^{-r}\|x_{i_0}\|^2|\mathbf{b}_1|^2 - rK_3^2} - rK_3 - 1)).$$

Note that, again, the upper bound obtained in this way is of the size of $(K_2^{-1}\log K_3)^{1/2}$.

6. Examples. In the examples of this section, the coordinates that we give for the various points Π are always $(x(\Pi), y(\Pi))$, i.e. they correspond to the model $y^2 = x^3 + Ax + B$, in the notation of Section 2. Also, we do not specially mention the values of the parameters u_0 and U_0; these can be easily calculated and never, in these examples, exceed 12.

EXAMPLE 1. Consider the equation

$$V^2 = Q(U) := U^4 - 8U^2 + 8U + 1 \tag{27}$$

and denote by E the elliptic curve defined by means of (27). Here,

$$a = 1, \quad b = 0, \quad c = -8, \quad d = 8, \quad e = 1,$$
$$A = \frac{-76}{3}, \quad B = \frac{1280}{27}, \quad \sigma = +1,$$
$$a_1 = 8, \quad a_2 = -24, \quad a_3 = 0, \quad a_4 = -4, \quad a_6 = 96,$$
$$\Delta_E = 2^{12} \cdot 17 = 69632, \quad j_E = \frac{438976}{17},$$
$$e_3 = -\frac{5}{3} - \sqrt{17} < x_0 = -\frac{2}{3} < -\frac{5}{3} + \sqrt{17} = e_2 < e_1 = \frac{10}{3},$$
$$\omega_1 = \frac{2\pi i}{M(\sqrt{e_1 - e_3}, \sqrt{e_2 - e_3})} = 2.133100331\ldots \cdot i,$$
$$\omega_2 = -\frac{2\pi}{M(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})} = -3.438877420\ldots,$$
$$\tau = 1.612149869\ldots i, \quad \omega = -\omega_2.$$

We apply Silverman's Theorem 1.1 [S2] to the Weierstrass minimal model of E, which Apecs found by application of Laska's algorithm:

$$Y_1^2 = X_1^3 + X_1^2 - 25X_1 + 39.$$

This gives (cf. (19)) $c_{11} = 3.19241$. Therefore, in order to find c_{10}, we must find an upper bound for $X_1(P)$. We have $X_1(P) = X(P) - 3$, hence

$$h(X_1(P)) \le \log\max\{|2\sqrt{Q(U)} - 3U^2 + 8U + 2|, U^2\} = \log U^2,$$

provided that $|U| \ge 4$. But we also have to check the analogous inequality that results if the coefficients b and d are replaced by $-b$ and $-d$, respectively (see the comment just after (12)). Again, $X_1(P) = X(P) - 3$ and the above inequality becomes

$$\begin{aligned} h(X_1(P)) &\le \log\max\{|2\sqrt{U^4 - 8U^2 - 8U + 1} - 3U^2 - 8U + 2|, U^2\} \\ &\le 2\log U + 0.6366, \end{aligned}$$

provided that $U > 10$. Also, if $U \ge 15$ then

$$\int_U^{+\infty} \frac{du}{\sqrt{u^4 - 8u^2 \pm 8u + 1}} < 1.02|U|^{-1};$$

hence $c_{10} = 0.6366$, $c_9 = 1.02$.

A basis, found by Apecs (*without assuming any of the standard conjectures*), is given by

$$P_1 = (-2/3, -8), \quad P_2 = (22/3, 16), \quad T = (10/3, 0),$$

where P_1, P_2 are the free generators and T is the generator of the torsion subgroup, of order 2. Apecs calculated, using Silverman's algorithm [S1], $\widehat{h}(P_1) = 0.317137308\ldots$, $\widehat{h}(P_2) = 0.480233071\ldots$ and a simple program based on MapleV and Apecs calculated the least eigenvalue of the regulator matrix, which is $c_1 = 0.237336274\ldots$ Since P_1 belongs to the compact component of $y^2 = x^3 + Ax + B$, we replace it by

$$R_1 = P_1 + Q_2 = \left(\frac{41}{6} - \frac{1}{2}\sqrt{17}, \frac{17}{2} - \frac{7}{2}\sqrt{17}\right),$$

where $Q_2 = (\sqrt{17} - 5/3, 0)$. We also put $R_2 = P_2$ and calculate

$$\phi(R_1) = 0.700983196\ldots, \qquad \phi(R_2) = 0.224621906\ldots$$

Since $x_0 \in (e_3, e_2)$, we also need the point P_0' (cf. (14)); we have

$$P_0 = (-2/3, 8) = -P_1, \qquad P_0' = P_0 + Q_2 = -P_1 - Q_2 = -R_1,$$

which immediately imply that $\phi(P_0') = \phi(-R_1) = 1 - \phi(R_1)$ and the right-hand side of (14), which we denoted by $\Phi(U)$ in Section 4, becomes

$$\begin{aligned}\Phi(U) &= (m_0 + s/2) + \phi(P_0') + m_1\phi(R_1) + m_2\phi(R_2)\\ &= (m_0 + 1 + s/2) + (m_1 - 1)\phi(R_1) + m_2\phi(R_2).\end{aligned}$$

From this we see that, in the notation of Section 5,

$$\frac{n_0}{d_0} = \frac{2m_0 + 2 + s}{2}, \qquad \frac{n_1}{d_1} = m_1 - 1, \qquad \frac{n_2}{d_2} = m_2$$

and, since $|m_0| \le 2M + 1$ (see just before (21)),

$$c_{12} = 4, \quad c_{13} = 5, \quad c_{12}' = 1, \quad c_{13}' = 1.$$

For the application of David's theorem we calculate:

$$h\left(\frac{A}{4}, \frac{B}{16}\right) = h\left(\frac{-19}{3}, \frac{80}{27}\right) = \log(9 \cdot 19),$$

$$h(j_E) = h\left(\frac{438976}{17}\right) = \log 438976, \qquad h_E = \log 438976.$$

Also, the coordinates of points R_1, R_2 belong to a quadratic field, hence $D = 2$ and

$$\frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = \frac{3\pi|\tau|}{2} = 7.597078, \qquad A_0 = h_E = 12.9922001,$$

$$\frac{3\pi\omega^2\phi(R_1)^2}{D|\omega_1|^2\Im\tau} = \frac{3\pi|\tau|\phi(R_1)^2}{2} = 3.733033, \quad A_1 = h_E,$$
$$\frac{3\pi\omega^2\phi(R_2)^2}{D|\omega_1|^2\Im\tau} = \frac{3\pi|\tau|\phi(R_2)^2}{2} = 0.383311, \quad A_2 = h_E$$

and $\mathcal{E} = 1.3077299e$. Finally,

$$c_4 = 2.9 \cdot 10^{24} \cdot 4^{18} \cdot 2^8 \cdot 4^{57.3} \cdot 1.26829^{-7} \cdot 2193.0479 = 6.6723 \cdot 10^{74},$$
$$c_5 = \log(D\mathcal{E}) = 1.96144, \quad c_6 = \log(D\mathcal{E}) + h_E = 14.953641,$$
$$c_7 = 3.42586, \quad c_8 = 15.482.$$

Now (23) implies $M < 2.15 \cdot 10^{41}$ and by the definition of $K_1, \ldots, K_4$ we have

$$K_1 = 9.9281, \quad K_2 = c_1, \quad K_3 = 2.15 \cdot 10^{41}, \quad K_4 = 2(K_3 + 1).$$

The hypothesis of Proposition 3 requires that $|\mathbf{b}_1| > 2\sqrt{6}K_4$, and this is satisfied if we choose $K_0 = 10^{128}$. Then, Proposition 3 gives the new bound $M \leq 29$. We repeat the process with $K_3 = 29$ and $K_0 = 10^8$ (of course, K_1 and K_2 remain the same) and get $M \leq 8$. This bound cannot be essentially improved further, therefore we give all points

$$m_1P_1 + m_2P_2, \quad m_1P_1 + m_2P_2 + T$$

in the range $0 \leq m_1 \leq 8, |m_2| \leq 8$, as an input to a simple program based in MapleV and Apecs, which transforms the (x, y)-coordinates of each one into its (U, V)-coordinates and accepts only those with U and V integers. The only accepted points turned out to be $(U, V) = (0, \pm 1)$. For the computation of c_9 and c_{10}, we have assumed that $|U| \geq 15$, therefore we had to check one by one all the values of U from -14 to 14 and this search gave no further solution. We have thus proved that: *the only integers satisfying* (27) *are* $(U, V) = (0, \pm 1)$.

Example 2. Consider Fermat's equation

$$V^2 = Q(U) := U^4 + 4U^3 + 10U^2 + 20U + 1 \tag{28}$$

(see [T1]) and denote by E the corresponding elliptic curve. Here

$$a = 1, \quad b = 4, \quad c = 10, \quad d = 20, \quad e = 1,$$
$$A = 128/3, \quad B = 5312/27, \quad \sigma = +1,$$
$$a_1 = 20, \quad a_2 = -90, \quad a_3 = 8, \quad a_4 = -4, \quad a_6 = 360,$$
$$\Delta_E = -2^4 \cdot 331 = -5296, \quad j_E = \frac{131072}{331},$$
$$e_1 = -3.556644723\ldots < x_0 = 16/3, \quad e_2, e_3 \notin \mathbb{R},$$
$$\omega_1 = \Omega_1 - \Omega_2, \ \omega_2 = \Omega_1 + \Omega_2, \ \Omega_1 = 1.502217471\ldots, \ \Omega_2 = 1.108711951\ldots \cdot i,$$
$$\tau = 0.294734582\ldots + 0.955579157\ldots \cdot i, \quad \omega = 2\Omega_1.$$

The minimal Weierstrass model for the elliptic curve E is

$$Y_1^2 = X_1^3 + X_1^2 + 3X_1 + 4 \qquad \big(X_1(P) = \tfrac{1}{4}X(P) + \tfrac{1}{2}\big).$$

Then, working as in Example 1, we calculate $c_{11} = 2.629582$, $c_{10} = 0.96$, $c_9 = 1.12$, the last two constants resulting from

$$\begin{aligned} h(X_1(P)) &= \log\max\{\sqrt{U^4 \pm 4U^3 + 10U^2 \pm 20U + 1} + U^2 \pm 10U + 1, 2U^2\} \\ &\le 2\log U + 0.96 \end{aligned}$$

and

$$\int\limits_U^{+\infty} \frac{du}{\sqrt{u^4 \pm 4u^3 + 10u^2 \pm 20u + 1}} < 1.12U^{-1},$$

respectively, provided that $U \ge 20$. A basis is given by (see [T1]) $P_1 = (4/3, -16)$, $P_2 = (16/3, 24)$; no torsion point other than $\mathcal{O}$ exists. We replace this basis by $P_1 - P_2$, P_2, because to this new basis there corresponds $K_2 = c_1$, better for the reduction process (i.e. greater). Thus, we take as a basis

$$\begin{gathered} R_1 = (-8/3, 8), \qquad R_2 = (16/3, 24); \\ \widehat{h}(R_1) = 0.176622454\ldots, \quad \widehat{h}(R_2) = 0.317960695\ldots, \\ c_1 = 0.173655878\ldots, \\ \phi(R_1) = 0.428683280\ldots, \quad \phi(R_2) = 0.251223446\ldots \end{gathered}$$

In this example, it is relation (13) that holds, hence we need the point P_0, which, as is straightforward to see, is equal to R_2 and the right-hand side of (13) becomes

$$\Phi(U) = m_0 + m_1\phi(R_1) + (m_2 + 1)\phi(R_2).$$

We see then that $c_{12} = 2$, $c_{13} = 2$, $c'_{12} = 1$, $c'_{13} = 1$.

For the application of David's theorem we calculate $h_E = h(j_E) = \log 131072$. Also, the coordinates of points R_1, R_2 are rational, hence $D = 1$ and

$$\frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 6\pi\frac{\Omega_1}{|\Omega_2|} = 25.5396654.$$

From this, we easily find that $A_0 = 25.5396654$, $A_1 = A_2 = h_E$, $\mathcal{E} = e$.

Finally,

$$c_4 = 2.9 \cdot 10^{24} \cdot 4^{18} \cdot 4^{57.3} \cdot 3546.21 = 2.225 \cdot 10^{73},$$

$$c_5 = 1, \quad c_6 = 12.7835021, \quad c_7 = 1.7556472, \quad c_8 = 13.056045.$$

Now (23) implies $M < 3.5 \cdot 10^{40}$; also

$$K_1 = 8.3547, \quad K_2 = c_1, \quad K_3 = 3.5 \cdot 10^{40}, \quad K_4 = K_3 + 1.$$

The hypothesis of Proposition 3 requires that $|\mathbf{b}_1| > 2\sqrt{6}K_4$, and this is satisfied if we choose $K_0 = 10^{125}$. Then, this proposition gives the new bound $M \le 33$ and by repeating the process with $K_3 = 33$ and

$K_0 = 10^9$ we get the bound $M \le 9$. Then a direct computer search, as in Example 1, shows that: *the only integers satisfying* (28) *are* $(U,V) = (-4,\pm 9), (-3,\pm 2), (0,\pm 1)$,
$(1,\pm 6)$.

In the examples that follow, we only give briefly all information needed for their solution. Bases for the Mordell–Weil groups of the corresponding curves have been easily calculated with the aid of Apecs 3.2, *unconditionally* (i.e. without assuming any of the standard conjectures).

Example 3. Consider the equation $3V^2 = 2U^4 - 2U^2 + 3$, solved by R. J. Stroeker and B. M. M. de Weger [SW]. On multiplying by 3 and replacing $3V$ by V we get the equation

$$V^2 = Q(U) := 6U^4 - 6U^2 + 9 \tag{29}$$

and we denote by E the corresponding elliptic curve. Here

$$\begin{gathered}
a = 6, \quad b = 0, \quad c = -6, \quad d = 0, \quad e = 3, \\
A = -228, \quad B = 848, \quad \sigma = +1, \quad be + d\sqrt{a} = 0, \\
a_1 = 0, \quad a_2 = -6, \quad a_3 = 0, \quad a_4 = -216, \quad a_6 = 1296, \\
\Delta_E = 2^{13} \cdot 3^7 \cdot 5^2 = 447897600, \qquad j_E = \frac{219488}{75}, \\
e_3 = -6\sqrt{6} - 2 < e_2 = 4 < e_1 = 6\sqrt{6} - 2 = x_0, \\
\omega_1 = 1.262713190\ldots \cdot i, \quad \omega_2 = -1.535696208\ldots, \\
\tau = 1.216187666\ldots \cdot i, \qquad \omega = -\omega_2.
\end{gathered}$$

The minimal Weierstrass model for the elliptic curve E is

$$y^2 = x^3 + Ax + B \qquad (x(P) = X(P) - 2);$$

from this we find, as in the previous examples, $c_{11} = 3.39514$, $c_{10} = 2.54766$, $c_9 = 0.41$, provided that $|U| \ge 15$. A basis is given by $P_1 = (2,20)$, $P_2 = (-2,36)$, with generator of the torsion group the point $T = (4,0)$. We replace this basis by

$$R_1 = P_1 + P_2 = (16,36), \qquad R_2 = P_2 + T = (34,180)$$

in order to get a greater value for c_1, which is $c_1 = 0.187960977\ldots$ Also,

$$\begin{gathered}
\widehat{h}(R_1) = 0.45320430\ldots, \qquad \widehat{h}(R_2) = 0.21172057\ldots; \\
\phi(R_1) = 0.36241206\ldots, \qquad \phi(R_2) = 0.22774550\ldots
\end{gathered}$$

In this example, it is relation (15) that holds, which is

$$\Phi(U) = (m_0 + s/2) + m_1\phi(R_1) + m_2\phi(R_2).$$

We see then that $c_{12} = 4$ and $c_{13} = 5$.

For the application of David's theorem we calculate $h_E = h(j_E) = \log 219488$. Also,

$$\frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 3\pi|\tau| = 11.46229871,$$

hence $A_0 = A_1 = A_2 = h_E$ and $\mathcal{E} = 1.0358e$.

Finally,

$$c_4 = 2.9\cdot 10^{24}\cdot 4^{18}\cdot 4^{57.3}\cdot 1.035174^{-7}\cdot 1860.4372 = 9.163\cdot 10^{72},$$
$$c_5 = \log\mathcal{E}, \quad c_6 = \log\mathcal{E} + h_E, \quad c_7 = 2.49962, \quad c_8 = 13.862405.$$

Now (23) implies $M < 2.35\cdot 10^{40}$; also

$$K_1 = 28.457, \quad K_2 = c_1, \quad K_3 = 2.35\cdot 10^{40}.$$

The hypothesis of Proposition 2 requires that $|\mathbf{b}_1| > 4\sqrt{6}K_3$ and this is satisfied if we choose $K_0 = 10^{125}$. Then, this proposition gives the new bound $M \le 32$ and by repeating the process with $K_3 = 32$ and $K_0 = 10^9$ we get the bound $M \le 10$. Then, a direct computer search, as in Example 1, shows that: *the only integers satisfying* (29) *are given by*

$$(|U|,|V|) = (0,3),(1,3),(2,9),(3,21),(6,87),(91,20283).$$

Example 4. Now we consider the equation $3u^4 - 2v^2 = 1$, solved by R. T. Bumby in an ingenious but complicated and quite *ad hoc* way (see [B]). We put $u = U+1$, $v = V/2$, so it suffices to solve in integers the equation

$$V^2 = Q(U) := 6U^4 + 24U^3 + 36U^2 + 24U + 4. \tag{30}$$

We denote by E the corresponding elliptic curve. Here

$$a = 6, \quad b = 24, \quad c = 36, \quad d = 24, \quad e = 2,$$
$$A = 48, \quad B = 0, \quad \sigma = +1,$$
$$a_1 = 12, \quad a_2 = 0, \quad a_3 = 96, \quad a_4 = -96, \quad a_6 = 0,$$
$$\Delta_E = -1728, \quad j_E = 1728,$$
$$e_1 = 0 < x_0 = 4\sqrt{6} + 12, \quad e_2, e_3 \notin \mathbb{R},$$
$$\Omega_1 = 1.408792103\ldots, \quad \Omega_2 = \Omega_1\cdot i,$$
$$\omega_1 = \Omega_1 - \Omega_2, \quad \omega_2 = \Omega_1 + \Omega_2, \quad \tau = i, \quad \omega = 2\Omega_1.$$

The minimal Weierstrass model for the elliptic curve E is

$$Y_1^2 = X_1^3 + 3X_1, \quad \big(X_1(P) = \tfrac{1}{4}X(P) + 3\big).$$

Then, $c_{11} = 1.69123$, and for $|U| \ge 20$, $c_{10} = 1.7927$ and $c_9 = 0.4566$.

The rank of E is 1 and $R_1 = P_1 = (4,16)$ is a generator of infinite order; the point $T = (0,0)$ is a generator of the torsion group, which is of order 2. Also, $c_1 = \widehat{h}(P_1) = 0.250591196\ldots$ and $\phi(R_1) = 0.301121610\ldots$

In this example, it is relation (13) that holds, so we need the point $P_0 = (4\sqrt{6}+12, 48+24\sqrt{6})$, for which we observe that $2P_0 = R_1$, hence (13) in our case becomes

$$\Phi(U) = (m_0 + s/2) + (m_1 + 1/2)\phi(R_1).$$

Then $c_{12} = 2$, $c_{13} = 5$, $c'_{12} = 2$ and $c'_{13} = 1$.

For the application of David's theorem we calculate

$$h_E = h(j_E) = \log 1728, \quad \frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 6\pi, \quad A_0 = 6\pi, \quad A_1 = h_E, \quad \mathcal{E} = e.$$

Finally,

$$c_4 = 2.9\cdot 10^{18}\cdot 4^8\cdot 3^{38.3}\cdot 140.52 = 5.01603\cdot 10^{43},$$
$$c_5 = 1, \quad c_6 = 1 + h_E, \quad c_7 = 1.8493972, \quad c_8 = 8.761075225$$

and now (23) implies $M < 5\cdot 10^{24}$; also

$$K_1 = 2.155, \quad K_2 = c_1, \quad K_3 = 5\cdot 10^{24}, \quad K_4 = 2K_3 + 1.$$

The hypothesis of Proposition 3 requires that $|\mathbf{b}_1| > 2K_4$ and this is satisfied if we choose $K_0 = 10^{52}$. Then, this proposition gives the new bound $M \le 15$ and by repeating the process with $K_3 = 15$ and $K_0 = 10^5$ we get the bound $M \le 5$. A direct computer search, as in Example 1, shows that: *the only integers satisfying* (30) *are* $(U,V) = (-4,\pm 22), (-2,\pm 2), (0,\pm 2), (2,\pm 22)$.

Example 5. Now we consider the equation $u^4 - 2u^2 + 4 = 3v^2$, a very difficult solution of which has been given by W. Ljunggren [L1]. We put $u = U + 1$, $v = V/3$, so it suffices to solve in integers the equation

$$V^2 = Q(U) := 3U^4 + 12U^3 + 12U^2 + 9. \tag{31}$$

We denote by E the corresponding elliptic curve. Here

$$a = 3, \quad b = 12, \quad c = 12, \quad d = 0, \quad e = 3,$$
$$A = -156, \quad B = 560, \quad \sigma = +1,$$
$$a_1 = 0, \quad a_2 = 12, \quad a_3 = 72, \quad a_4 = -108, \quad a_6 = -1296,$$
$$\Delta_E = 2^{14}3^8, \quad j_E = \frac{35152}{9},$$
$$e_3 = -14 < e_2 = 4 < e_1 = 10 < x_0 = 6\sqrt{3} + 4,$$
$$\omega_1 = -1.376409401\ldots\cdot i, \quad \omega_2 = 1.760787652\ldots,$$
$$\tau = 1.279261571\ldots\cdot i, \quad \omega = \omega_2.$$

The minimal Weierstrass model for the elliptic curve E is

$$y^2 = x^3 + Ax + B \quad (x(P) = X(P) + 4).$$

Then, $c_{11} = 4.34$, and for $|U| \geq 20$, $c_{10} = 2.7394$ and $c_9 = 0.6455$. The rank of E is 1 and $P_1 = (2, 16)$ is a free generator; since it belongs to the compact part of $E(\mathbb{R})$, we replace it by $P_1 + Q_2 = (2, 16) + (4, 0)$. Thus,

$$R_1 = (58, 432), \quad c_1 = \widehat{h}(R_1) = 0.539636932\ldots, \quad \phi(R_1) = 0.149818526\ldots$$

The only torsion point on $E_0(\mathbb{Q})$ is $T = (10, 0)$, of order 2. In this example, it is relation (13) that holds, so we need also the point $P_0 = (6\sqrt{3} + 4, 36)$, for which we observe that $2P_0 + T = R_1$, hence $2\phi(P_0) = \phi(R_1) + 1/2$ and (13) in our case becomes

$$\varPhi(U) = \frac{4m_0 + 2s + 1}{4} + \frac{2m_1 + 1}{2}\phi(R_1).$$

Then $c_{12} = 4$, $c_{13} = 11$, $c'_{12} = 2$ and $c'_{13} = 1$.

For the application of David's theorem we calculate

$$h_E = h(j_E) = \log 35152, \quad \frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 3\pi|\tau|,$$
$$A_0 = 3\pi|\tau|, \quad A_1 = h_E, \quad \mathcal{E} = e.$$

Finally,

$$c_4 = 2.9 \cdot 10^{18} \cdot 4^8 \cdot 3^{38.3} \cdot 126.2033344 = 4.505 \cdot 10^{43},$$
$$c_5 = 1, \quad c_6 = 1 + h_E, \quad c_7 = 2.55817, \quad c_8 = 12.02943$$

and now (23) implies $M < 4.54 \cdot 10^{24}$; also

$$K_1 = 110.632, \quad K_2 = c_1, \quad K_3 = 4.54 \cdot 10^{24}, \quad K_4 = 2(2K_3 + 1).$$

The hypothesis of Proposition 3 requires that $|\mathbf{b}_1| > 2K_4$ and this is satisfied if we choose $K_0 = 10^{52}$. Then, this proposition gives the new bound $M \leq 11$ and one more reduction step with $K_3 = 11$ and $K_0 = 10^5$ implies $M \leq 4$. A direct computer search shows that: *the only integers satisfying* (31) *are* $(U, V) = (-3, \pm 6), (-2, \pm 3), (0, \pm 3), (1, \pm 6), (12, \pm 291)$.

Example 6. Next, we consider the rather well known equation $2u^4 - 1 = v^2$. A very complicated solution has been given by W. Ljunggren [L2]; recently, R. Steiner and the author [StT] gave a conceptually much simpler solution, based on the theory of linear forms in (ordinary) logarithms. Here we offer one more solution.

We put $u = U + 1$, $v = V$, and solve the equation

$$V^2 = Q(U) := 2U^4 + 8U^3 + 12U^2 + 8U + 1. \tag{32}$$

We denote by E the corresponding elliptic curve. In this example

$$a = 2, \quad b = 8, \quad c = 12, \quad d = 8, \quad e = 1,$$
$$A = 8, \quad B = 0, \quad \sigma = +1,$$
$$a_1 = 8, \quad a_2 = -4, \quad a_3 = 16, \quad a_4 = -8, \quad a_6 = 32,$$

$$\Delta_E = -2^{15}, \quad j_E = 1728,$$
$$e_1 = 0 < x_0 = 2\sqrt{2}+4, \quad e_2, e_3 \notin \mathbb{R},$$
$$\Omega_1 = 2.204878798\ldots, \quad \Omega_2 = \Omega_1 i,$$
$$\omega_1 = \Omega_1 - \Omega_2, \quad \omega_2 = \Omega_1 + \Omega_2, \quad \tau = i, \quad \omega = 2\Omega_1.$$

Minimal Weierstrass model: $y^2 = x^3 + Ax + B$, $(x(P) = X(P) + 4)$. Then,

$$c_{11} = 2.557661 \quad \text{and for } |U| \ge 20, \quad c_{10} = 2.01801, \quad c_9 = 0.791.$$

The rank of E is 1 and $P_1 = (1,3)$ is a free generator; thus,

$$R_1 = (1,3), \quad c_1 = \widehat{h}(R_1) = 0.608709032\ldots, \quad \phi(R_1) = 0.341556449\ldots$$

Generator of the torsion group : $T = (0,0)$, of order 2. We are in case (13):

$$P_0 = (2\sqrt{2}+4, 8\sqrt{2}+8), \quad 2P_0 = P_1,$$
$$\Phi(U) = \frac{2m_0+s}{2} + \frac{2m_1+1}{2}\phi(R_1),$$
$$c_{12} = 2, \quad c_{13} = 5, \quad c'_{12} = 2, \quad c'_{13} = 1.$$

For the application of David's theorem we calculate

$$h_E = h(j_E) = \log 1728, \quad \frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 6\pi = A_0, \quad A_1 = h_E, \quad \mathcal{E} = e,$$
$$c_4 = 2.9\cdot 10^{18}\cdot 4^8\cdot 3^{38.3}\cdot 140.518161 = 5.016\cdot 10^{43},$$
$$c_5 = 1, \quad c_6 = 1 + h_E, \quad c_7 = 1.8493972, \quad c_8 = 8.76108.$$

Relation (23) implies $M < 3.5\cdot 10^{24}$; also

$$K_1 = 6.3496, \quad K_2 = c_1, \quad K_3 = 3.5\cdot 10^{24}, \quad K_4 = 2K_3+1, \quad K_0 = 10^{51}.$$

First reduction: $M \le 10$, second reduction: $M \le 4$. *The only integers satisfying* (32) *are* $(U,V) = (-14,\pm 239), (-2,\pm 1), (0,\pm 1), (12,\pm 239)$.

Example 7. Finally, we consider the equation $u^4 + 2u^2 - 1 = 2v^2$ [L3]. We put $u = U+1$, $v = V/2$, and solve the equation

$$V^2 = Q(U) := 2U^4 + 8U^3 + 16U^2 + 16U + 4. \tag{33}$$

We denote by E the corresponding elliptic curve. In this example

$$a = 2, \quad b = 8, \quad c = 16, \quad d = 16, \quad e = 2,$$
$$A = \frac{32}{3}, \quad B = \frac{1280}{27}, \quad \sigma = +1,$$
$$a_1 = 8, \quad a_2 = 0, \quad a_3 = 32, \quad a_4 = -32, \quad a_6 = 0,$$
$$\Delta_E = -2^8, \quad j_E = 2^7,$$
$$e_1 = -8/3 < x_0 = 4\sqrt{2} + 16/3, \quad e_2, e_3 \notin \mathbb{R},$$
$$\Omega_1 = 2.018230827\ldots, \quad \Omega_2 = 1.37367687\ldots\cdot i,$$
$$\omega_1 = \Omega_1 - \Omega_2, \quad \omega_2 = \Omega_1 + \Omega_2, \quad |\tau| = 1, \quad \omega = 2\Omega_1.$$

Minimal Weierstrass model: $Y_1^2 = X_1^3 + X_1^2 + X_1 + 1$ $\big(X_1(P) = \frac{1}{4}X(P) + 1\big)$.

$$c_{11} = 2.28301 \quad \text{and for } |U| \geq 20, \quad c_{10} = 1.0181, \quad c_9 = 0.7911.$$

The rank of E is 1 and $P_1 = (4/3, 8)$ is a free generator; thus,

$$R_1 = (4/3, 8), \quad c_1 = \widehat{h}(R_1) = 0.2161655\ldots, \quad \phi(R_1) = 0.295679873\ldots$$

Generator of the torsion group: $T = (-8/3, 0)$, of order 2. We are in case (13):

$$P_0 = (4\sqrt{2} + 16/3, 16\sqrt{2} + 16), \quad 2P_0 = P_1,$$
$$\Phi(U) = \frac{2m_0 + s}{2} + \frac{2m_1 + 1}{2}\phi(R_1),$$
$$c_{12} = 2, \quad c_{13} = 5, \quad c'_{12} = 2, \quad c'_{13} = 1.$$

For the application of David's theorem we calculate

$$h_E = h(j_E) = \log 128, \quad \frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 6\pi\frac{\Omega_1}{|\Omega_2|} = A_0, \quad A_1 = h_E, \quad \mathcal{E} = e,$$
$$c_4 = 2.9 \cdot 10^{18} \cdot 4^8 \cdot 3^{38.3} \cdot 134.37266 = 4.7966 \cdot 10^{43},$$
$$c_5 = 1, \quad c_6 = 1 + h_E, \quad c_7 = 1.8494, \quad c_8 = 6.252312.$$

Relation (23) implies $M < 3.8 \cdot 10^{24}$; also

$$K_1 = 3.1975, \quad K_2 = c_1, \quad K_3 = 3.8 \cdot 10^{24}, \quad K_4 = 2K_3 + 1, \quad K_0 = 10^{51}.$$

First reduction: $M \leq 17$, second reduction: $M \leq 6$. *The only integers satisfying* (33) *are* $(U, V) = (-4, \pm 14), (-2, \pm 2), (0, \pm 2), (2, \pm 14)$.

7. Appendix: Lower bound for the linear form in elliptic logarithms. In this paper we need to know a non-trivial lower bound for a linear form of the shape

$$L = \frac{p_0}{q_0}\omega + \frac{p_1}{q_1}u_1 + \ldots + \frac{p_k}{q_k}u_k,$$

where ω is the fundamental real period of the Weierstrass $\wp$ function associated with the eliptic curve

$$E : y^2 = q(x) := x^3 + Ax + B, \quad A, B \in \mathbb{Q},$$

and the u_i's are *elliptic logarithms* of points $\Pi_i \in E(\overline{\mathbb{Q}})$ (in our case $u_i = \phi(\Pi_i)\omega$ and the Π_i's are the basic points $R_1, \ldots, R_r$ and, possibly P_0 or P'_0); actually, these coordinates belong to a number field of degree $D \leq 3$.

We view the numerators p_i as *unknown* integers for the absolute value of which we know a "very large" upper bound; in contrast, the denominators q_i are "very small", *explicitly known* integers.

As always in this paper, let e_1, e_2, e_3 be the (distinct) roots of $q(x) = 0$, with $e_1 \in \mathbb{R}$ and $e_1 > e_2 > e_3$ if all three are real.

First we give formulas for a pair of fundamental periods ω_1, ω_2 of $\wp$. In general, for any pair (x,y) of real numbers, let $M(x,y)$ denote the *arithmetic-geometric mean* of x, y (see [Cx]). Then (see the Appendix of [ST]),

- If $q(x)=0$ has three real roots, we can take

$$\omega_1=\frac{2\pi}{M(\sqrt{e_1-e_3},\sqrt{e_1-e_2})},\qquad \omega_2=\frac{2\pi i}{M(\sqrt{e_1-e_3},\sqrt{e_2-e_3})}.$$

- If $q(x)=0$ has only one real root, we can take

$$\omega_1=\Omega_1+\Omega_2,\quad \omega_2=\Omega_1-\Omega_2,$$

where

$$\Omega_1=\frac{\pi}{M\big(\sqrt[4]{3e_1^2+A},\frac{1}{2}\sqrt{3e_1+2\sqrt{3e_1^2+a}}\big)},$$
$$\Omega_2=\frac{\pi i}{M\big(\sqrt[4]{3e_1^2+A},\frac{1}{2}\sqrt{-3e_1+2\sqrt{3e_1^2+a}}\big)}.$$

By making a linear unimodular transformation to (ω_1,ω_2), if necessary, we may always assume that $\tau:=\omega_2/\omega_1$ satisfies

$$|\tau|\ge 1,\quad \Im\tau>0,\quad -1/2<\Re\tau\le 1/2\quad \text{with } \Re\tau\ge 0 \text{ if } |\tau|=1.$$

From ω_1,ω_2 we can also easily find the minimum positive real period ω.

We define now the *height* of a rational n-tuple. Let, in general, $(a_1/b_1,\ldots,a_n/b_n)$, $n\ge 1$, be an n-tuple of rational numbers a_i/b_i in lowest terms $(b_i>0)$ and let $b>0$ be the least common multiple of the b_i's. Then we define

$$h\bigg(\frac{a_1}{b_1},\ldots,\frac{a_n}{b_n}\bigg)=\max\bigg\{b,\frac{b|a_1|}{b_1},\ldots,\frac{b|a_n|}{b_n}\bigg\}$$

(actually, this is the *absolute logarithmic height* of the point $(1,a_1/b_1,\ldots,a_n/b_n)\in\mathbb{P}^n(\mathbb{Q})$).

Let $j_E=2^83^3A^3/(4A^3+27B^2)$ be the j-invariant of E and define

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

Finally, choose $A_0,A_1,\ldots,A_k$ and $\mathcal{E}$ such that

$$A_0\ge\max\bigg\{h_E,\frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau}\bigg\},$$
$$A_i\ge\max\bigg\{h_E,\frac{3\pi\omega^2\phi(\Pi_i)^2}{D|\omega_1|^2\Im\tau},\widehat{h}(\Pi_i)\bigg\},\quad i=1,\ldots,k,$$

and

$$e\le\mathcal{E}\le e\cdot\min\bigg\{\frac{|\omega_1|}{\omega}\cdot\sqrt{\frac{DA_0\Im\tau}{3\pi}},\frac{|\omega_1|}{\omega\phi(\Pi_i)}\cdot\sqrt{\frac{DA_i\Im\tau}{3\pi}},i=1,\ldots,k\bigg\}.$$

The following theorem is a direct consequence of a result due to S. David (Théorème 2.1 of [Da]). David's theorem is the explicit version of a general (effective but not explicit) result of N. Hirata-Kohno (Corollaire 2.16 of [HK]).

THEOREM 5. *Let* $N = \max_{0\le i\le k} |p_i|$. *If* $L \ne 0$, *then either*

$$N < \max\{\exp(eh), |q_i|, \exp(A_i/D),\ i = 0, \ldots, k\},$$

or

$$|L| > \exp(-c_4(\log N + c_5)(\log\log N + c_6)^{k+2}),$$

where

$$c_4 = 2.9 \cdot 10^{6k+12} D^{2k+4} 4^{2(k+1)^2} (k+2)^{2k^2+13k+23.3} (\log \mathcal{E})^{-2k-3} \prod_{i=0}^{k} A_i,$$

$$c_5 = \log(D\mathcal{E}), \quad c_6 = \log(D\mathcal{E}) + h_E.$$

References

[B] R. T. Bumby, *The diophantine equation* $3x^4 - 2y^2 = 1$, Math. Scand. 21 (1967), 144–148.

[Cn] I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra 145 (1992), 463–467.

[Cx] D. A. Cox, *The arithmetic-geometric mean of Gauss*, Enseign. Math. 30 (1984), 275–330.

[Da] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. 62 Soc. Math. France (Suppl. to Bull. Soc. Math. France 123 (3) (1995)), to appear.

[Di] L. E. Dickson, *History of the Theory of Numbers*, Vol. II, Chelsea, New York, 1971.

[GPZ] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. 68 (1994), 171–192.

[G] R. K. Guy, *Reviews in Number Theory 1973–83*, Vol. 2A, Amer. Math. Soc., Providence, R.I., 1984.

[HK] N. Hirata-Kohno, *Formes linéaires de logarithmes de points algébriques sur les groupes algébriques*, Invent. Math. 104 (1991), 401–433.

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

[LV] W. J. LeVeque, *Reviews in Number Theory 1940–72*, Vol. 2, Amer. Math. Soc., Providence, R.I., 1974.

[L1] W. Ljunggren, *Einige Sätze über unbestimmte Gleichungen von der Form* $Ax^4 + Bx^2 + C = Dy^2$, Vid.-Akad. Skrifter I (9) (1942), 53 pp.

[L2] —, *Zur Theorie der Gleichung* $X^2 + 1 = DY^4$, Avh. Norske Vid. Akad. Oslo I (5) (1942), 27 pp.

[L3] —, *Proof of a theorem of de Jonquières*, Norsk Mat. Tidsskrift 26 (1944), 3–8 (in Norwegian).

[S1] J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.

[S2] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, ibid. 55 (1990), 723–743.

[StT] R. Steiner and N. Tzanakis, *Simplifying the solution of Ljunggren's equation* $X^2 + 1 = 2Y^4$, J. Number Theory 37 (1991), 123–132.

[Str] R. J. Stroeker, *On the sum of consecutive cubes being a perfect square*, Compositio Math. 97 (1995), 295–307.

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

[SW] R. J. Stroeker and B. M. M. de Weger, *On a quartic Diophantine equation*, Proc. Edinburgh Math. Soc., to appear.

[T1] J. Top, *Fermat's "primitive solutions" and some arithmetic of elliptic curves*, Indag. Math. 4 (1993), 211–222.

[T2] —, *Examples of elliptic quartics with many integral points*, private communication, September 1994.

[dW] B. M. M. de Weger, *Algorithms for diophantine equations*, CWI Tract 65, Centre for Mathematics and Computer Science, Amsterdam, 1989.

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

Department of Mathematics
University of Crete
P.O. Box 470
714 09 Iraklion, Greece
E-mail: tzanakis@knosos.math.uch.gr

Received on 10.7.1995
and in revised form on 17.9.1995 (2824)